TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

Destinataire:

NONNENMACHER, Bernard
Gemplus S.C.A
Parc d'activités de Gémenos
Avenue du Pic de Bertagne
F-13881 Gémenos Cedex
FRANCE

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Date d'expédition (jour/mois/année)	
24 octobre 2000 (24.10.00)	
Référence du dossier du déposant ou du mandataire GEM 603	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR99/02918	**Date du dépôt international** (jour/mois/année) 25 novembre 1999 (25.11.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

[X] le déposant [ ] l'inventeur [ ] le mandataire [ ] le représentant commun

Nom et adresse	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)
GEMPLUS S.C.A. Avenue du Pic de Bertagne Parc d'Activités de Gémenos F-13881 Gémenos Cedex FRANCE	FR	FR
	no de téléphone	
	no de télécopieur	
	no de téléimprimeur	

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

[ ] la personne [X] le nom [ ] l'adresse [ ] la nationalité [ ] le domicile

Nom et adresse	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)
GEMPLUS Avenue du Pic de Bertagne Parc d'Activités de Gémenos F-13881 Gémenos Cedex FRANCE	FR	FR
	no de téléphone	
	no de télécopieur	
	no de téléimprimeur	

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

[X] à l'office récepteur
[ ] à l'administration chargée de la recherche internationale
[X] à l'administration chargée de l'examen préliminaire international
[ ] aux offices désignés concernés
[X] aux offices élus concernés
[ ] autre destinataire:

Bureau international de l'OMPI **34, chemin des Colombettes** **1211 Genève 20, Suisse**	Fonctionnaire autorisé: Sean Taylor
no de télécopieur (41-22) 740.14.35	no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 24 août 2000 (24.08.00)	
Demande internationale no PCT/FR99/02918	**Référence du dossier du déposant ou du mandataire** GEM 603
Date du dépôt international (jour/mois/année) 25 novembre 1999 (25.11.99)	**Date de priorité** (jour/mois/année) 14 janvier 1999 (14.01.99)
Déposant PAILLIER, Pascal	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

12 juillet 2000 (12.07.00)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé
Alejandro HENNING

no de téléphone: (41-22) 338.83.38

INTERNATIONAL SEARCH REPORT

Intl. Jonal Application No
PCT/FR 99/02918

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YASUKO GOTOH ET AL: "A METHOD FOR RAPID RSA KEY GENERATION" SYSTEMS & COMPUTERS IN JAPAN, vol. 21, no. 8, 1 January 1990 (1990-01-01), pages 11-20, XP000177817 ISSN: 0882-1666 page 12, right-hand column, line 12 -page 13, left-hand column, line 12	1,16

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 2000	18/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numéro de publication internationale:
H04L 9/30	A1	WO 00/42734
		(43) Date de publication internationale: 20 juillet 2000 (20.07.00)

(21) Numéro de la demande internationale: PCT/FR99/02918

(22) Date de dépôt international: 25 novembre 1999 (25.11.99)

(30) Données relatives à la priorité:
99/00341 14 janvier 1999 (14.01.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: PAILLIER, Pascal [FR/FR]; 37, cours de Vincennes, F–75020 Paris (FR).

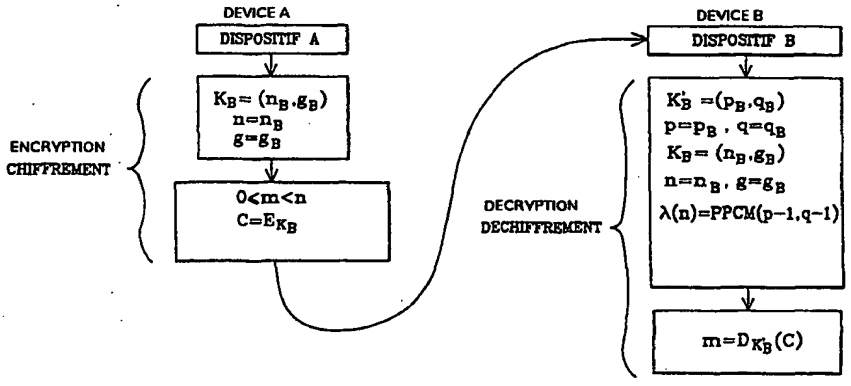
(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A, Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: PUBLIC AND PRIVATE KEY CRYPTOGRAPHIC METHOD

(54) Titre: PROCEDE CRYPTOGRAPHIQUE A CLES PUBLIQUE ET PRIVEE



(57) Abstract

The invention concerns a cryptographic method for generating public keys (K) and private keys (K') which consists in: selecting two distinct first numbers p and q, of neighbouring value and calculating the number n equal to the product of p.q; calculating the lowest common multiple of the numbers (p–1) and (q–1): $\lambda(n) = PPCM(p-1, q-1)$; determining a number g, $0<g\leq n^2$ which verifies the two following conditions: a) g is invertible modulo n^2; and b) $ord(g,n^2) = 0 \bmod n$. The public key is formed by the parameters n and g and its private key is formed by the parameters p, q and $\lambda(n)$or by the parameters p and q. An encryption method for a number m representing a message, $0\leq m<n$ consists in calculating the cryptogram c $0\ g^m \bmod n^2$.

(57) Abrégé

Un procédé cryptographique comprend un procédé de génération de clés publique (K) et privée (K') comprenant la sélection de deux nombres premiers p et q distincts, de taille voisine et le calcul du nombre n égal au produit p.q; le calcul du plus petit commun multiple des nombres (p−1) et (q−1): $\lambda(n)$=PPCM(p−1, q−1); la détermination d'un nombre g, $0 \leq g < n^2$ qui vérifie les deux conditions suivantes: a) g est inversible modulo n^2 et b) $ord(g,n^2) = 0 \bmod n$. La clé publique est formée par les paramètres n et g et sa clé privée est formée par les paramètres p, q et $\lambda(n)$ ou par les paramètres p et q. Un procédé de chiffrement d'un nombre m représentatif d'un message, $0 \leq < n$ consiste à calculer le cryptogramme $c=g^m \bmod n^2$.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCEDE CRYPTOGRAPHIQUE A CLES PUBLIQUE ET PRIVEE

La présente invention concerne un procédé cryptographique à clés publique et privée. Il est utilisable dans toutes les applications dans lesquelles il est nécessaire d'assurer la confidentialité des messages transmis sur un canal quelconque et/ou d'identifier avec certitude un dispositif avec lequel on échange des messages.

La confidentialité de messages transmis entre deux dispositifs A et B sur un canal de communication quelconque est obtenue en chiffrant l'information transmise pour la rendre inintelligible aux personnes à qui elle n'est pas destinée. L'identification certaine d'un dispositif est lui basé le calcul de la signature numérique d'un message.

En pratique, deux types de procédé cryptographique peuvent être utilisés celui dit symétrique, à clés secrètes, dont un exemple bien connu est le DES...celui dit asymétrique, utilisant une paire de clés publique et privée et décrit dans *« New directions in Cryptography » IEEE Transactions on Information Theory, nov. 1976, par* MM Diffie et Hellman. Un exemple bien connu de procédé asymétrique est le RSA, du nom de ses inventeurs Ronald Rivest, Adi Shamir et Léonard Adleman. On peut trouver une description de ce procédé RSA dans le brevet américain US 4, 405, 829.

Dans l'invention, on s'intéresse plus particulièrement à un procédé cryptographique asymétrique.

Un procédé de chiffrement selon un procédé cryptographique asymétrique consiste principalement, pour un émetteur A qui veut envoyer confidentiellement un message à un destinataire B à prendre connaissance, par exemple dans un annuaire, de la clé publique K_B du destinataire B, à appliquer le procédé de chiffrement E sur le message m à transmettre en utilisant cette clé publique, et à envoyer au destinataire B, le cryptogramme c résultant: $c= E_{KB}(m)$.

Ce procédé consiste principalement pour le destinataire B, à recevoir le cryptogramme c, et à le déchiffrer pour obtenir le message d'origine m, en appliquant le procédé de déchiffrement D sur le cryptogramme c en utilisant la clé privée K'b qu'il est le seul à connaître: m=Dk'b(c).

Selon ce procédé n'importe qui peut envoyer un message chiffré au destinataire B, mais seul ce dernier est capable de le déchiffrer.

On utilise habituellement un procédé cryptographique asymétrique pour la génération/vérification de signature. Dans ce contexte, un utilisateur qui veut prouver son identité utilise une clé privée, connue de lui seul, pour produire une signature numérique s d'un message m, signature qu'il transmet au dispositif destinataire. Ce dernier met en oeuvre la vérification de la signature en utilisant la clé publique de l'utilisateur. Tout dispositif a ainsi la capacité de vérifier la signature d'un utilisateur, en prenant connaissance de la clé publique de cet utilisateur et en l'appliquant dans l'algorithme de vérification. Mais seul l'utilisateur concerné a la capacité

de générer la bonne signature utilisant sa clé privée. Ce procédé est par exemple beaucoup utilisé dans les systèmes de contrôle d'accès ou de transactions bancaires. Il est en général couplé à l'utilisation d'un procédé de chiffrement, pour chiffrer la signature avant de la transmettre.

Pour cette génération/vérification de signatures numériques, on peut utiliser en pratique des procédés cryptographiques asymétriques dédiés à cette application, tel le DSA *(Digital Signature Algorithm)*, qui correspond à un standard américain proposé par le *US National Institute of Standards and Technology*. On peut en outre utiliser le RSA qui a la propriété de pouvoir être utilisé aussi bien en chiffrement qu'en génération de signature.

Dans l'invention, on s'intéresse à un procédé cryptographique qui peut être utilisé pour le chiffrement des messages et pour la génération de signature numérique. Dans l'état actuel de la technique, seul le RSA, dont il existe de nombreuses variantes de mise en oeuvre, offre cette double fonctionnalité.

Le RSA comprend une étape de génération des clés publique K et privée K' pour un dispositif donné dans laquelle on procède de la façon suivante :

- on choisit deux grands nombres premiers p et q, distincts.
- on calcule leur produit n=p.q.
- on choisit un nombre e premier avec le plus petit commun multiple de (p-1)(q-1). En pratique, e est souvent pris égal à 3.

La clé publique K est alors formée par le couple de paramètres (n,e) et la clé secrète K' est formée par le couple de paramètres (p,q).

En choisissant p et q de grande taille, leur produit n est aussi de grande taille. N est donc très difficile à factoriser : on est assuré que l'on ne pourra pas retrouver la clé secrète K'=(p,q) à partir de la connaissance de n .

Le procédé de chiffrement d'un nombre m représentant un message M, $0 \leq m < n$ consiste alors, à effectuer le calcul suivant :

$c = E_B(m) = m^e \bmod n$

au moyen de la clé publique K=(n,e).

Le procédé de déchiffrement consiste lui dans le calcul inverse suivant :

$m = c^d \bmod (n)$

au moyen de la clé privée K'=(p,q), gardée secrète, où

$$d = \frac{1}{e} \bmod (p-1)(q-1).$$

On a vu que le RSA a la particularité d'être utilisable pour la vérification de signature. Le procédé correspondant de génération de signature par un utilisateur A consiste à utiliser le procédé de déchiffrement avec la clé secrète pour produire la signature s d'un nombre m représentatif d'un message. On a ainsi : $s = m^d \bmod n$.

Cette signature s est transmise à un destinataire B. Ce dernier, qui connaît m (par exemple, A transmet s et m), vérifie la signature en effectuant l'opération inverse, c'est à dire en utilisant le procédé de chiffrement avec la clé

publique de l'émetteur A. C'est à dire qu'il calcule $v=s^e \bmod n$, et vérifie $v=m$.

En général, pour améliorer la sécurité d'un tel procédé de vérification de signature, on applique préalablement une fonction de hachage sur le nombre m avant de calculer la signature, qui peut consister en des permutations de bits et/ou une compression.

Quand on parle de message M à chiffrer ou à signer, il s'agit bien sûr de messages numériques, qui peuvent résulter d'un codage numérique préalable. Ce sont en pratique des chaînes de bits, dont la taille binaire (nombre de bits) peut être variable.

Or un procédé de cryptographie comme le RSA est tel qu'il permet de chiffrer avec la clé publique (n,e) n'importe quel nombre entre 0 et n-1. Pour l'appliquer à un message M de taille quelconque, il faut donc en pratique couper ce message en une suite de nombres m qui vérifieront chacun la condition $0 \leq m < n$. On applique alors le procédé de chiffrement sur chacun de ces nombres. Dans la suite, on s'intéresse donc à l'application du procédé cryptographique sur un nombre m représentatif du message M. m peut-être égal à M, ou en n'être qu'une partie. On désigne alors indifféremment dans la suite par m le message ou un nombre représentatif du message.

Un objet de l'invention, est un procédé de cryptographie asymétrique différent de ceux basés sur le RSA.

Un objet de l'invention, est un procédé reposant sur d'autres propriétés, qui puisse s'appliquer aussi bien en chiffrement de messages qu'en génération de signatures.

Un objet de l'invention, est un procédé de cryptographie qui permette, dans certaines configurations, un temps de traitement plus rapide.

Telle que caractérisée, l'invention concerne un procédé cryptographique selon la revendication 1.

L'invention sera mieux comprise à la lecture de la description suivante , faite à titre indicatif et nullement limitatif de l'invention et en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma fonctionnel d'un système de communication cryptographique de type asymétrique;
- la figure 2 est un schéma fonctionnel d'un dispositif communiquant utilisé dans un système de communication cryptographique selon l'invention;
- la figure 3 est un organigramme d'une session de chiffrement/déchiffrement de messages utilisant le procédé cryptographique selon l'invention; et
- la figure 4 est un organigramme d'une session de génération/vérification de signature utilisant le procédé cryptographique selon l'invention.

Pour bien comprendre l'invention, il est nécessaire de faire quelques préliminaires mathématiques.

Dans la description, on utilise les notations mathématiques suivantes :

(1) Si a est un entier relatif et b un entier strictement positif, a mod b (a modulo b) est le résidu modulaire de a relativement à b et désigne l'unique entier strictement inférieur à b tel que b divise (a - a mod b).

(2) (Z/bZ) désigne l'ensemble des résidus modulo b et forme un groupe pour l'addition modulaire .

(3) $(Z/bZ)^*$ désigne l'ensemble des entiers inversibles modulo b et forme un groupe pour la multiplication modulaire.

(4) L'ordre d'un élément a de $(Z/bZ)^*$ est le plus petit entier naturel ord(a,b) tel que $a^{ord(a,b)}=1 \bmod b$.

(5) PPCM (a,b) désigne le plus petit commun multiple de a et b.

(6)PGCD(a,b) désigne le plus grand commun diviseur de a et b.

(7) $\lambda(a)$désigne la fonction de Carmichael de a. Si $a=p.q$, $\lambda(a)=PPCM(p-1, q-1)$.

(8) On note $x=TRC(a_1,...a_k, b_1,...b_k)$ l'unique solution, obtenue par la mise en oeuvre du Théorème du Reste Chinois bien connu, du système d'équations modulaires suivant :

$x=a_1 \bmod b_1$

$x= a_2 \bmod b_2$

...

$x= a_k \bmod b_k$.

où les entiers a_i et b_i sont donnés et où, $\forall i,j$ avec $i\neq j$, $PGCD(b_i, b_j)=1$.

(9) On rappelle que la taille binaire d'un nombre a est le nombre de bits sur lesquels a s'écrit.

Soit maintenant un nombre n, entier, de taille arbitraire. L'ensemble $Un=\{x<n^2 / x=1 \bmod n\}$ est un sous-groupe multiplicatif de $(Z/n^2Z)^*$.

Soit alors $\log_n$ la fonction définie sur l'ensemble Un par :

$$\log_n(x) = \frac{x-1}{n}$$

Cette fonction a la propriété suivante :

$\forall\ x \in Un,\ \forall\ y \in Un,\ \log_n(xy \bmod n^2) = \log_n(x) + \log_n(y) \bmod n$.

Par conséquent, si g est un nombre entier arbitraire appartenant à Un, on a pour tout nombre m, $0 \leq m < n$:

$\log_n(g^m \bmod n^2) = m.\log_n(g) \bmod n$.

Cette propriété mathématique est à la base du procédé de cryptographie mis en oeuvre dans l'invention qui va maintenant être décrite.

La figure 1 représente un système de communication cryptographique, utilisant un procédé cryptographique asymétrique. Il comprend des dispositifs communiquants, dans l'exemple A et B, sur un canal de communication 1. Dans l'exemple, on a représenté un canal bidirectionnel. Chaque dispositif contient une paire de clés publique K et privée K'.

Les clés publiques sont par exemple publiées dans un fichier public 2 tel qu'un annuaire, que chaque dispositif peut consulter. Dans ce fichier public, on trouvera ainsi la clé publique K_A du dispositif A et celle K_B du dispositif B.

La clé privée K' de chaque dispositif est conservée par lui de façon secrète, typiquement dans une zone sécurisée de mémoire non volatile. Le dispositif A contient ainsi en mémoire secrète sa clé privée K'_A et le dispositif B contient ainsi en mémoire secrète sa clé privée K'_B. Ils

conservent aussi leur clé publique, mais dans une zone mémoire sans protection d'accès particulière.

Dans un tel système, le dispositif A peut chiffrer un message m en un cryptogramme c_A en utilisant la clé publique K_B du dispositif B; ce dernier peut déchiffrer c_A en utilisant sa clé privée K'_B, qu'il conserve secrètement. Inversement, , le dispositif B peut chiffrer un message m en un cryptogramme c_B en utilisant la clé publique K_A du dispositif A; ce dernier peut déchiffrer c_B en utilisant sa clé privée K'_A, qu'il conserve secrètement.

Typiquement, chaque dispositif comprend au moins, comme représenté sur la figure 2, des moyens de traitement 10, c'est à dire une unité centrale de traitement (CPU), comprenant notamment différents registres R pour le calcul, une interface de communication 11 avec le canal de communication, et des moyens de mémorisation. Ces moyens de mémorisation comprennent généralement une mémoire programme 12 (ROM, EPROM, EEPROM) et une mémoire de travail (RAM) 13 . En pratique, chaque dispositif conserve ses données secrètes dans une zone d'accès sécurisée 120 prévue en mémoire programme et ses données publiques dans une zone d'accès normal de cette mémoire. La mémoire de travail permet de conserver momentanément, le temps nécessaire aux calculs, des messages à chiffrer, des cryptogrammes à déchiffrer, ou encore des résultats de calculs intermédiaires.

Les moyens de traitement et de mémorisation permettent ainsi d'exécuter des programmes liés à l'application, et notamment d'effectuer les calculs correspondant à la mise en oeuvre du procédé de

cryptographie pour le chiffrement /déchiffrement de messages et/ou la génération/vérification de signatures selon l'invention. Ces calculs comprennent notamment, comme on le verra de façon détaillée dans la suite, des élévations à la puissance, des résidus et inversions modulaires .

Les dispositifs peuvent encore comprendre un générateur 14 de nombre aléatoire ou pseudo-aléatoire r , qui peut intervenir dans les calculs précités, dans certaines variantes de réalisation. Ce générateur est encadré en pointillé sur la figure 2, pour indiquer qu'il n'est pas nécessaire à la réalisation de toutes les variantes de réalisation selon l'invention.

Tous ces moyens du dispositif sont connectés à un bus d'adresses et de données 15.

De tels dispositifs utilisés dans l'invention sont bien connus, et correspondent par exemple à ceux qui sont utilisés dans les systèmes de communication cryptographique de l'état de la technique, mettant en oeuvre le RSA. Ils ne seront donc pas détaillés plus avant. Un exemple pratique de système de communication cryptographique, est le système formé des serveurs bancaires et des cartes à puce, pour la gestion de transactions financières. Mais il existe de nombreuses autres applications, telle les applications liées au commerce électronique .

Un premier mode de réalisation de l'invention va maintenant être détaillé, au regard de l'organigramme représenté sur la figure 3.

Cet organigramme représente une séquence de communication entre un dispositif A et un dispositif B sur un canal de communication 20. Ces dispositifs comprennent au moins les moyens de traitement, de mémorisation et de communication décrits en relation avec la figure 2.

Le procédé de cryptographie selon l'invention comprend un procédé de générations des clés publique K et privée K'.

Selon l'invention, ce procédé de génération des clés publique et privée d'un dispositif comprend les étapes suivantes :

- sélection de deux grands nombres premiers p et q distincts et de taille voisine;
- calcul du nombre n égal au produit p.q;
- calcul du nombre $\lambda(n)=PPCM(p-1 , q-1)$, c'est à dire de la fonction de Carmichael du nombre n;
- détermination d'un nombre g, $0 \leq g < n^2$, qui remplisse les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2)=0 \bmod n$.

Cette condition b) indique que l'ordre du nombre g dans l'ensemble $(Z/n^2Z)^*$ des nombres entiers de 0 à n^2 est un multiple non nul du nombre n, selon les notations définies plus haut.

La clé publique K est alors formée par le nombre n et le nombre g. La clé privée est formée par les nombres p,q et $\lambda(n)$ ou seulement par les nombres p et q, $\lambda(n)$ pouvant être recalculé à chaque utilisation de la clé secrète.

On génère selon ce procédé les clés publique et privée de chaque dispositif. Cette génération peut-être effectuée, selon les dispositifs considérés et les applications, par les dispositifs eux-mêmes ou par un organe externe.

Chaque dispositif, par exemple le dispositif A, contient donc en mémoire sa clé publique $K_A = (n_A, g_A)$ et, de façon secrète, sa clé privée $K'_A = (p_A, q_A)$.

En outre, les clés publiques sont mises dans un fichier accessible au public.

On verra ci-dessous qu'il est avantageux de choisir $g=2$, lorsque c'est possible, c'est à dire, lorsque $g=2$ remplit les conditions a) et b) du procédé de génération de signature selon l'invention.

Un procédé de chiffrement selon un premier mode de réalisation du procédé cryptographique de l'invention mis en oeuvre dans le dispositif A consiste alors, pour l'envoi d'un message au dispositif B, dans la réalisation des étapes suivantes, avec $0 \leq m < n$:

- renseignement des paramètres n et g du procédé de chiffrement mis en oeuvre par le dispositif A par la clé publique K_B du deuxième dispositif B : $n = n_B$, $g = g_B$.
- calcul du cryptogramme $c = g^m \bmod n^2$, et
- transmission du cryptogramme c sur le canal de communication.

Le procédé de chiffrement selon un premier mode de réalisation de l'invention consiste donc à prendre le paramètre g de la clé publique, à l'élever à la puissance m, et à calculer le résidu modulaire relativement à n^2. On

notera que dans le RSA, c'est le message m qui est élevé à la puissance alors que dans l'invention, le message m est utilisé comme exposant.

Le dispositif B qui reçoit le message chiffré, c'est à dire le cryptogramme c, met alors en oeuvre un procédé de déchiffrement selon l'invention avec les paramètres de sa clé privée. Ce procédé de déchiffrement comprend le calcul suivant :

- calcul du nombre m tel que

$$m = \frac{\log_n(c^{\lambda(n)} \bmod n^2)}{\log_n(g^{\lambda(n)} \bmod n^2)} \bmod n$$

où

$$\log_n(x) \quad \frac{x-1}{n} .$$

Si g=2, on voit que le calcul d'élévation de g à la puissance est facilité. On prendra donc de préférence g=2, toutes les fois où ce sera possible. En d'autres termes, le procédé de génération des clés commencera par essayer si g=2 remplit les conditions a) et b).

Différentes variantes de calcul du procédé de déchiffrement peuvent être mises en oeuvre, qui permettent, lorsque le dispositif doit déchiffrer un grand nombre de cryptogrammes, de précalculer certaines quantités et de les conserver de façon secrète dans le dispositif. Une contrepartie est que la zone mémoire secrète (zone 120 sur la figure 2) du dispositif doit être plus étendue, puisqu'elle doit alors contenir des paramètres supplémentaires en plus des paramètres p et q. Ceci n'est pas sans influencer le choix de mise en oeuvre d'une variante ou d'une autre. En effet, la réalisation

d'une zone de mémoire sécurisée est coûteuse, et donc de capacité (mémoire) généralement limitée, notamment dans les dispositifs dits à bas côuts (par exemple, certains types de cartes à puce).

Dans une première variante de mise en oeuvre du procédé de déchiffrement, on prévoit que le dispositif, B en l'occurrence, précalcule une fois pour toutes la quantité :

$$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

et la conserve secrète en mémoire.

Ainsi, on réduit d'autant le temps nécessaire au déchiffrement de chacun des messages reçus par le dispositif. En effet, lorsque que le dispositif B exécute une instance de cette variante du procédé de déchiffrement, il ne lui reste plus qu'à calculer :

$$m = \log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n.$$

Dans une deuxième variante de mise en oeuvre du procédé de déchiffrement selon l'invention, on prévoit d'utiliser le Théorème du Reste Chinois, pour une meilleure efficacité (rapidité du calcul).

Dans une instance de cette deuxième variante du procédé de déchiffrement, le dispositif effectue les calculs (de déchiffrement) suivants :

1 $m_p = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

2 $m_q = \log_q(c^{q-1} \bmod q^2)\log_p(g^{q-1} \bmod q^2)^{-1} \bmod q$

3 $m = TRC(m_p, m_q, p, q)$,

où

$\log_p(x)$ $\dfrac{x-1}{p}$ et

$$\log_q(x) \quad \frac{x-1}{q}$$

Dans ce cas, on peut en outre prévoir, dans les cas où le dispositif est amené à déchiffrer un très grand nombre de messages, que le dispositif précalcule une fois pour toutes les quantités suivantes :

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ et

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

Le dispositif doit alors conserver ces quantités comme données secrètes.

Le calcul effectué lors d'une instance du procédé de déchiffrement devient :

1. $m_p = \log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $m_q = \log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
3. $m = TRC(m_p, m_q, p, q)$.

Comme déjà précisé, toutes ses variantes de calcul de déchiffrement sont intéressantes lorsque le dispositif est amené à déchiffrer un très grand nombre de messages, et que le gain en temps de traitement compense la plus grande capacité mémoire de la zone sécurisée pour conserver toutes les données secrètes. Le choix de l'une ou l'autre variante dépend en pratique de l'application considérée et des contraintes de coûts et de temps de traitement à concilier.

Un deuxième mode de réalisation de l'invention comprend l'utilisation d'un nombre aléatoire, fournit par un générateur de nombre aléatoire (ou pseudo-aléatoire), dans le procédé de chiffrement, en sorte que pour un même message m à transmettre, le cryptogramme calculé c sera

différent à chaque fois. La sécurité du système de communication est donc plus grande. Le procédé de déchiffrement est inchangé.

Ce deuxième mode de réalisation de l'invention comprend deux variantes.

Dans une première variante, le cryptogramme c est obtenu par le calcul suivant : $c=g^{m+nr} \bmod n^2$.

Dans une deuxième variante, le cryptogramme c est obtenu par le calcul suivant : $c=g^m r^n \bmod n^2$.

Cette deuxième variante nécessite en pratique un temps de traitement plus long que la première, mais elle offre une plus grande sécurité.

Dans un troisième mode de réalisation de l'invention, on impose que l'ordre de g dans $(Z/nZ)^*$ soit un entier de petite taille, ceci étant obtenu par une mise en oeuvre du procédé de génération des clés différente.

Avec une telle condition sur l'ordre du paramètre g, on réduit la complexité du calcul du procédé de déchiffrement qui devient en pratique quadratique (c'est à dire en x^2) par rapport à la taille du nombre n.

Dans ce troisième mode de réalisation de l'invention, le procédé de génération des clés publique et privée est alors le suivant :

- sélection en secret, d'un entier u et de deux grands nombres premiers p et q distincts et de taille voisine tels que u divise (p-1) et divise (q-1).
- calcul du nombre n égal au produit p.q;
- calcul du nombre $\lambda(n)=PPCM(p-1 , q-1)$, c'est à dire de la fonction de Carmichael du nombre n;

- détermination d'un nombre h, $0 \leq h < n^2$, qui remplisse les deux conditions suivantes :

a) h est inversible modulo n^2 et

b) $ord(h,n^2) = 0 \bmod n$.

- calcul du nombre $g = h^{\lambda(n)/u} \bmod n^2$.

La clé publique K est alors formée par le nombre n et le nombre g. La clé privée est constituée par les entiers (p,q,u) conservés secrètement dans le dispositif.

De préférence, on choisit h=2, lorsque c'est possible (c'est à dire si h=2 remplit les conditions a) et b), pour faciliter le calcul de g.

On notera que si u =PGCD(p-1,q-1), il n'est pas nécessaire de conserver ce nombre qui peut-être retrouvé par le dispositif à partir de p et q.

De préférence, on choisira u premier, pour améliorer la sécurité du procédé, et de petite taille, typiquement 160 bits. En choisissant une petite taille pour u, on verra que l'on facilite le calcul de déchiffrement.

Dans ce troisième mode de réalisation, la mise en oeuvre du procédé de chiffrement pour chiffrer un message m est identique à celle précédemment décrite dans le premier mode de réalisation de l'invention, le cryptogramme étant égal à $c = g^m \bmod n^2$.

On peut aussi calculer le cryptogramme c en utilisant une variable aléatoire r selon la première variante du deuxième mode de réalisation de l'invention précédemment décrit. r est alors un entier aléatoire, de même taille que u et le cryptogramme est obtenu par le calcul suivant : $c = g^{m+nr} \bmod n^2$.

Le cryptogramme c calculé selon l'une ou l'autre mise en oeuvre précédente du procédé de chiffrement est envoyé au dispositif B qui doit le déchiffrer. La mise en oeuvre du procédé de déchiffrement par le dispositif B qui reçoit le message est un peu différente.

En effet, le calcul effectué dans le dispositif dans une instance de déchiffrement, pour retrouver le nombre m à partir du cryptogramme c devient le suivant :

$$m = \frac{\log_n(c^u \bmod n^2)}{\log_n(g^u \bmod n^2)} \bmod n.$$

On peut appliquer comme précédemment des variantes de calcul qui permettent d'accélérer le temps de traitement nécessaire.

Dans une première variante, on va ainsi précalculer une fois pour toutes la quantité :

$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$

et la conserver secrètement en mémoire.

Lors d'une instance de déchiffrement d'un cryptogramme c reçu, le dispositif n'a plus qu'à effectuer le calcul suivant :

$m = \log_n(c^u \bmod n^2).\beta_{n,g} \bmod n.$

Dans une deuxième variante, on met en oeuvre le Théorème du Reste Chinois, en utilisant les fonctions $\log_p$ et $\log_q$ déjà vues pour effectuer le calcul de déchiffrement.

Lors d'une instance de cette variante du procédé de déchiffrement du cryptogramme c reçu, le dispositif effectue alors les calculs suivants :

1. $m_p=\log_p(c^u \bmod p^2)\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q=\log_q(c^u \bmod q^2)\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = TRC(m_p,m_q,p,q)$.

Dans une troisième variante, on accélère encore le temps de traitement nécessaire au déchiffrement du cryptogramme c selon la deuxième variante, en précalculant les quantités suivantes :

$\beta_{p,g}=\log_p(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g}=\log_q(g^u \bmod q^2)^{-1} \bmod q$

et en les conservant de façon secrète dans le dispositif.

Lors d'une instance de calcul de cette troisième variante du procédé de déchiffrement du cryptogramme c reçu, le dispositif n'a alors plus qu'à effectuer les calculs suivants :

1. $m_p=\log_p(c^u \bmod p^2)\ \beta_{p,g} \bmod p$
2. $m_q=\log_q(c^u \bmod q^2)\ \beta_{q,g} \bmod q$
3. $m = TRC(m_p,m_q,p,q)$.

Dans un quatrième mode de réalisation de l'invention, le procédé de chiffrement et le procédé de déchiffrement sont tels qu'ils présentent la particularité d'être des permutations sur le groupe des entiers modulo n^2. En d'autres termes, si le message m s'exprime sur k bits, le cryptogramme c obtenu en appliquant le procédé de chiffrement sur m et la signature s obtenue en appliquant le procédé de déchiffrement sur m sont aussi sur k bits.

Cette particularité confère au procédé cryptographique la propriété supplémentaire de pouvoir

être utilisé aussi bien en chiffrement/déchiffrement qu'en génération/vérification de signature. Dans ce cas, le procédé de déchiffrement est employé comme procédé de génération de signature et le procédé de chiffrement comme procédé de vérification de signature.

Dans ce quatrième mode de réalisation, le procédé de génération des clés publique et privée est le même que celui du premier mode de réalisation de l'invention : $K=(n,g)$ et $K'=(p,q,\lambda(n))$ ou $K'=(p,q)$.

Si le dispositif A veut envoyer un message m chiffré au dispositif B, il se procure la clé publique (n,g) de ce dernier, puis dans une instance du procédé de chiffrement, effectue alors les calculs suivants, appliqué au nombre m, $0 \leq m < n^2$:

1. $m_1 = m \bmod n$
2. $m_2 = (m-m1)/n$ (division euclidienne)
3. $c = g^{m1}\, m_2^{\,n} \bmod n^2$.

C'est ce cryptogramme c qui est envoyé au dispositif B.

Ce dernier doit donc lui appliquer le procédé de déchiffrement correspondant, pour retrouver m_1, m_2 et finalement m. Ce procédé de déchiffrement selon le quatrième mode de réalisation de l'invention consiste à effectuer les calculs suivants :

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w = cg^{-m1} \bmod n$.
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

Comme précédemment, des variantes du procédé de déchiffrement selon ce quatrième mode de réalisation de l'invention sont applicables, qui permettent de réduire le temps de traitement nécessaire pour déchiffrer un message donné. Elles sont intéressantes lorsque le dispositif a un grand nombre de cryptogrammes à déchiffrer.

Une première variante consiste à précalculer les quantités suivantes :

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ et

$\gamma_n = 1/n \bmod \lambda(n)$

que le dispositif B calcule une fois pour toutes et conserve secrètes en mémoire.

A chaque nouvelle instance de déchiffrement d'un cryptogramme c reçu selon cette première variante, le dispositif B n'a plus qu'à effectuer les calculs suivants :

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^{\gamma n} \bmod n$.
4. $m = m_1 + nm_2$.

Dans une deuxième variante de la mise en oeuvre du procédé de déchiffrement selon le quatrième mode de réalisation, on utilise le Théorème du Reste Chinois.

Le dispositif qui veut déchiffrer un cryptogramme c selon cette deuxième variante effectue alors les calculs successifs suivants :

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{\,1/q \bmod p-1} \bmod p$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2)\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

5. $w_q = c g^{-m_{1,q}} \bmod q$
6. $m_{2,q} = w_q^{1/p \bmod q-1} \bmod q$
7. $m_1 = TRC(m_{1,p}, m_{2,p}, p, q)$.
8. $m_2 = TRC(m_{1,q}, m_{2,q}, p, q)$.
9. $m = m_1 + pqm_2$.

Dans une troisième variante, pour améliorer encore temps de traitement du déchiffrement de cette deuxi variante, le dispositif B peut précalculer une fois toutes les quantités suivantes :

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

et les conserver secrètes en mémoire.

Le dispositif qui veut déchiffrer un cryptogra selon cette troisième variante n'a plus qu'à effect calculs suivants:

1. $m_{1,p} = \log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $w_p = c g^{-m_{1,p}} \bmod p$
3. $m_{2,p} = w_p^{\gamma p} \bmod p$
4. $m_{1,q} = \log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
5. $w_q = c g^{-m_{1,q}} \bmod q$
6. $m_{2,q} = w_q^{\gamma q} \bmod q$
7. $m_1 = TRC(m_{1,p}, m_{2,p}, p, q)$.
8. $m_2 = TRC(m_{1,q}, m_{2,q}, p, q)$.
9. $m = m_1 + pqm_2$.

Le quatrième mode de réalisation de l'i vient d'être décrit permet de faire de la

vérification de signature. Comme représenté sur l'organigramme de la figure 4, si le dispositif B doit générer une signature s d'un nombre m représentatif d'un message vers le dispositif A, il applique comme procédé de génération de la signature, le procédé de déchiffrement avec sa clé privée : $s=D_{K'B}(m)$.

Le dispositif A qui reçoit la signature s et qui connaît le message m, vérifie que la signature est bonne en calculant la quantité v obtenue en appliquant le procédé de chiffrement sur la signature s avec la clé publique : $v=E_{KB}(s)$. Si la signature est bonne, on a v=m.

Toutes les variantes de mise en oeuvre du procédé de déchiffrement de ce quatrième mode de réalisation qui permettent d'accélérer le temps de traitement sont aussi bien applicable en génération/vérification de signature.

L'invention qui vient d'être décrite est applicable dans tous les systèmes où l'on veut pouvoir chiffrer et/ou signer des messages. Elle permet d'élargir les possibilités d'adaptation aux différentes applications, selon que l'on recherche plus de sécurité, ou une vitesse de traitement accrue. A cet égard, on notera que le troisième mode de réalisation de l'invention, dont la complexité de calcul est seulement quadratique (fonction du carré de la taille de n) offre un réel avantage en terme de vitesse, dans la mesure où tous les procédés de l'état de la technique ont un ordre de complexité supérieur (fonction du cube de la taille de n). Un tel avantage intéresse plus particulièrement toutes les applications utilisant des dispositifs portables, tels les

cartes à puces et plus particulièrement les dispositifs à bas coûts.

Enfin, toute personne expérimentée dans la technique concernée par l'invention comprendra que des modifications dans la forme et/ou des détails peuvent être effectués sans sortir de l'esprit de l'invention. En particulier on peut chiffrer la signature, ou encore appliquer une fonction de hachage au message m avant de calculer sa signature.

REVENDICATIONS

1. Procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication, la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, le procédé de génération comprenant les étapes suivantes :

- sélection de deux nombres premiers p et q distincts, de taille voisine;
- calcul du nombre n égal au produit p.q;

caractérisé en ce que ledit procédé comprend en outre les étapes suivantes :

- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$
- détermination d'un nombre g , $0 \leq g < n^2$ qui vérifie les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2) = 0 \bmod n$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et $\lambda(n)$ ou par les paramètres p et q.

2. Procédé de génération selon la revendication 1, caractérisé en ce qu'il consiste à prendre g=2, si g vérifie les dites conditions a) et b).

3. Système de communication cryptographique à clés publique et privée générées selon la revendication 1 ou 2, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant au moins une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique (n_B, g_B) du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de chiffrement,

- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

4. Système selon la revendication 3 , caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$.

5. Système selon la revendication 3, caractérisé en ce que le dispositif mettant en oeuvre le procédé de

chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c=g^m r^n \bmod(n^2)$.

6. Système selon l'une des revendications 3 à 5, caractérisé en ce que le deuxième dispositif (B) met en oeuvre un procédé de déchiffrement, pour déchiffrer ledit cryptogramme c, et qui comprend la réalisation du calcul

$$m= \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

où $\log_n(x)= \dfrac{x-1}{n}$.

7. Système selon la revendication 6, caractérisé en ce qu'un dispositif (B) mettant en oeuvre ledit procédé de déchiffrement, précalcule la quantité :

$$\alpha_{n,g}= \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

et la conserve secrètement.

8. Système selon la revendication 6, caractérisé en ce que dans une instance dudit procédé de déchiffrement un dispositif effectue les étapes de calcul suivantes, utilisant le Théorème du Reste Chinois TRC :

$$m_p=\log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p.$$

$$m_q=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$$

$m=TRC(m_p,m_q,p,q)$., où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x)= \frac{x-1}{i} .$$

9. Système selon la revendication 8, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ et

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

et les conserve secrètement.

10. Système de communication cryptographique à clés publique et privée générées selon la revendication 1 ou 2, comprenant un canal de communication (20) et des dispositifs communiquant (A,B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n^2$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $K_B=(n_B,g_B)$ du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de déchiffrement,
- et réalisation des calculs suivants :

1. $m_1 = m \bmod n$
2. $m_2 = (m-m1)/n$
3. $c = g^{m1}\, m_2{}^n \bmod n^2$.

ledit cryptogramme c étant transmis sur le canal de communication.

11. Système selon la revendication 10, caractérisé en ce que en ce que le deuxième dispositif (B) reçoit le cryptogramme c et met en oeuvre un procédé de déchiffrement, pour déchiffrer ledit cryptogramme qui comprend la réalisation des étapes suivantes de calcul :

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

12. Système selon la revendication 11, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement, précalcule les quantités suivantes :

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ et

$\gamma_n= 1/n \bmod \lambda(n)$

et les conserve secrètement.

13. Système selon la revendication 11, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif effectue les étapes de calcul suivant, en utilisant le Théorème du Reste Chinois :

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$.
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$
7. $m_1=TRC(m_{1,p},m_{2,p},p,q)$.
8. $m2=TRC(m_{1,q},m_{2,q},p,q)$.

9. $m = m_1 + pqm_2$, où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x) = \frac{x-1}{i}$$

14. Système selon la revendication 13, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif précalcule les quantités suivantes :

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

et les conserve secrètement.

15. Système selon l'une quelconque des revendications 11 à 14, dans lequel le procédé de déchiffrement est utilisé pour calculer la signature s d'un message m et le procédé de chiffrement est utilisé pour vérifier ladite signature.

16. Procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication (20), la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, procédé de génération caractérisé en ce qu'il comprend les étapes suivantes :

- sélection d'un nombre u et de deux nombres premiers p et q distincts, de taille voisine, tels que u divise (p-1) et divise (q-1);

- calcul du nombre n égal au produit p.q;

- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$

- détermination d'un nombre h , $0 \leq h < n^2$ qui vérifie les deux conditions suivantes :

a) h est inversible modulo n^2 et

b) $ord(h,n^2) = 0 \bmod n$,

- calcul du nombre $g=h^{\lambda(n)/u} \bmod n^2$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et u.

17. Procédé selon la revendication 16, caractérisé en ce qu'il consiste à choisir h=2, si les conditions a) et b) sont remplies.

18. Procédé selon la revendication 16, caractérisé en ce que u est le plus grand commun diviseur de (p-1), (q-1).

19. Procédé selon la revendication 16, caractérisé en ce que u est un nombre premier.

20. Système de communication cryptographique à clés publique et privée générées selon l'une des revendications 16 à 19, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans

un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $(n,g)_B$ du deuxième dispositif (B) pour renseigner les paramètres n et g du procédé de chiffrement,
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

21. Système selon la revendication 20, caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$.

22. Système selon la revendication 20 ou 21, caractérisé en ce que le deuxième dispositif met en oeuvre un procédé de déchiffrement du cryptogramme reçu c, comprenant la réalisation du calcul suivant :

$$m = \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n.$$

23. Procédé selon la revendication 22, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule la quantité :

$$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$$

et la conserve secrètement .

24. Système selon la revendication 22, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif effectue les étapes de calcul suivantes, en utilisant le Théorème du reste chinois :

1. $m_p=\log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$.
2. $m_q=\log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$.
3. $m = TRC(m_p,m_q,p,q)$, où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x)= \frac{x-1}{i}.$$

25. Système selon la revendication 24, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes :

$\beta_{p,g}=\log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g}=\log_n(g^u \bmod q^2)^{-1} \bmod q$

et les conserve secrètement.

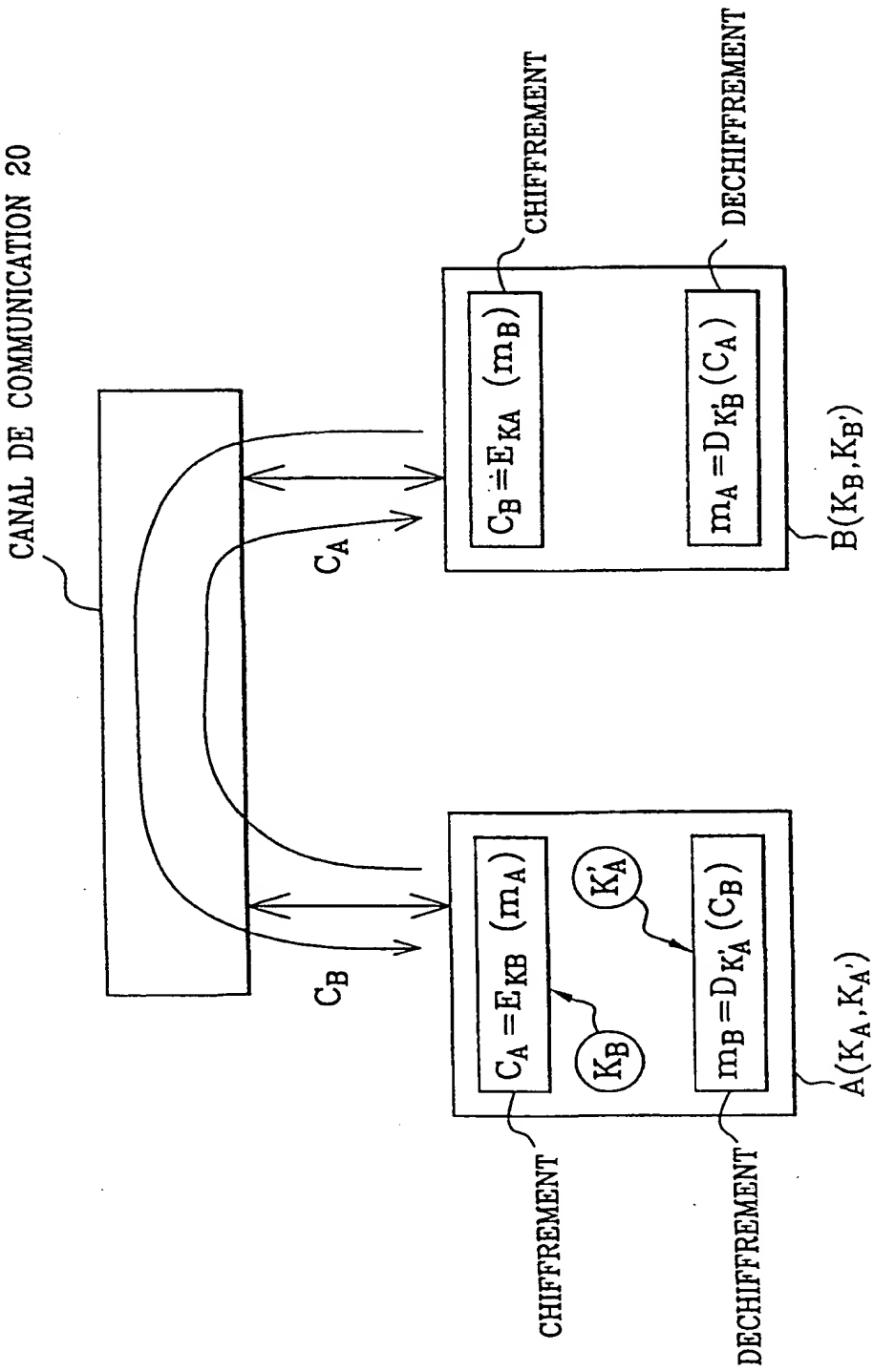

CANAL DE COMMUNICATION 20
CHIFFREMENT
DECHIFFREMENT
$C_B = E_{KA}(m_B)$
$m_A = D_{K'B}(C_A)$
C_A
$B(K_B, K_{B'})$
$C_A = E_{KB}(m_A)$
$m_B = D_{K'A}(C_B)$
K_B
K'_A
C_B
$A(K_A, K_{A'})$
CHIFFREMENT
DECHIFFREMENT

FIG.1

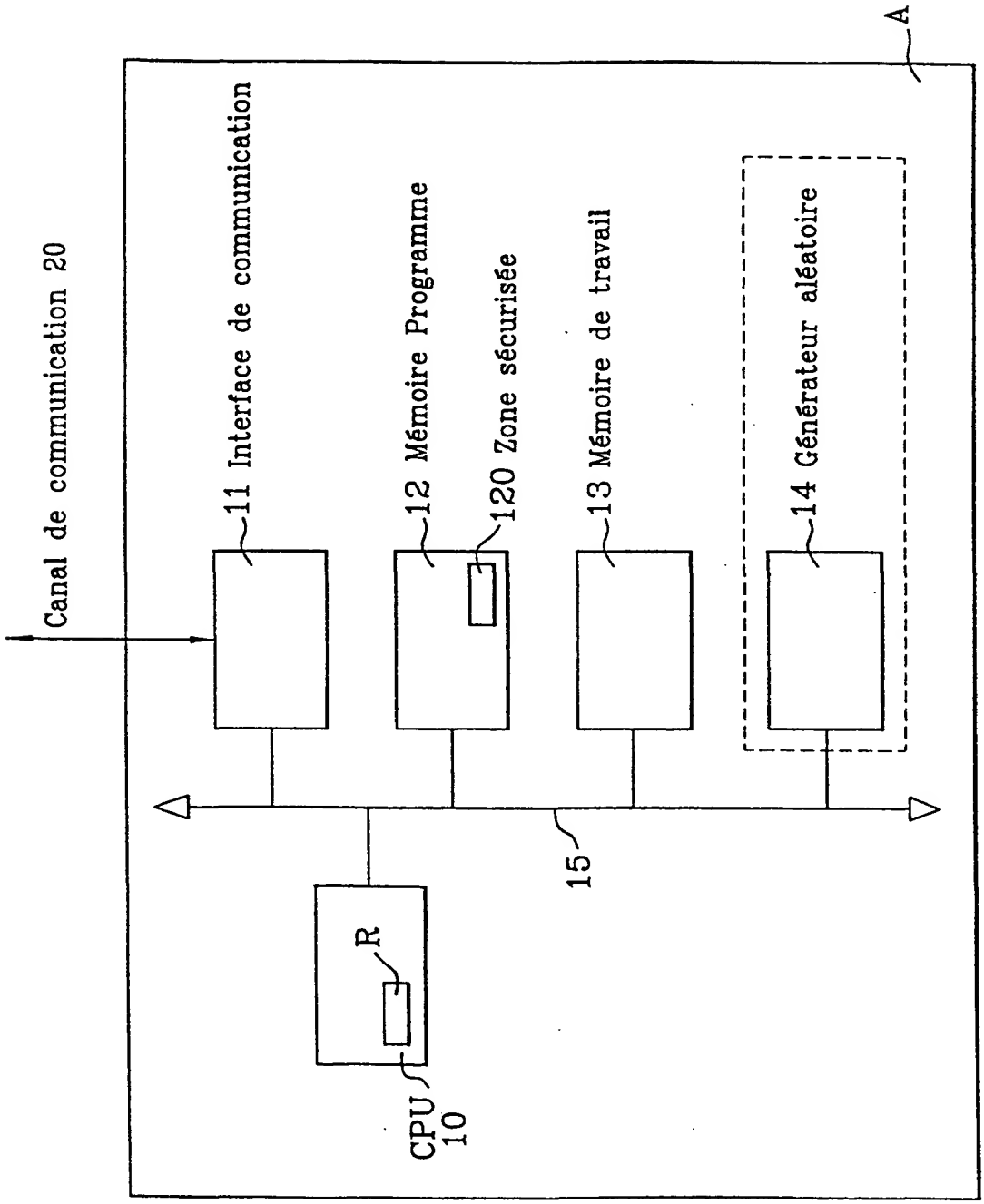

A
Canal de communication 20
11 Interface de communication
12 Mémoire Programme
120 Zone sécurisée
13 Mémoire de travail
14 Générateur aléatoire
15
R
CPU
10

FIG.2

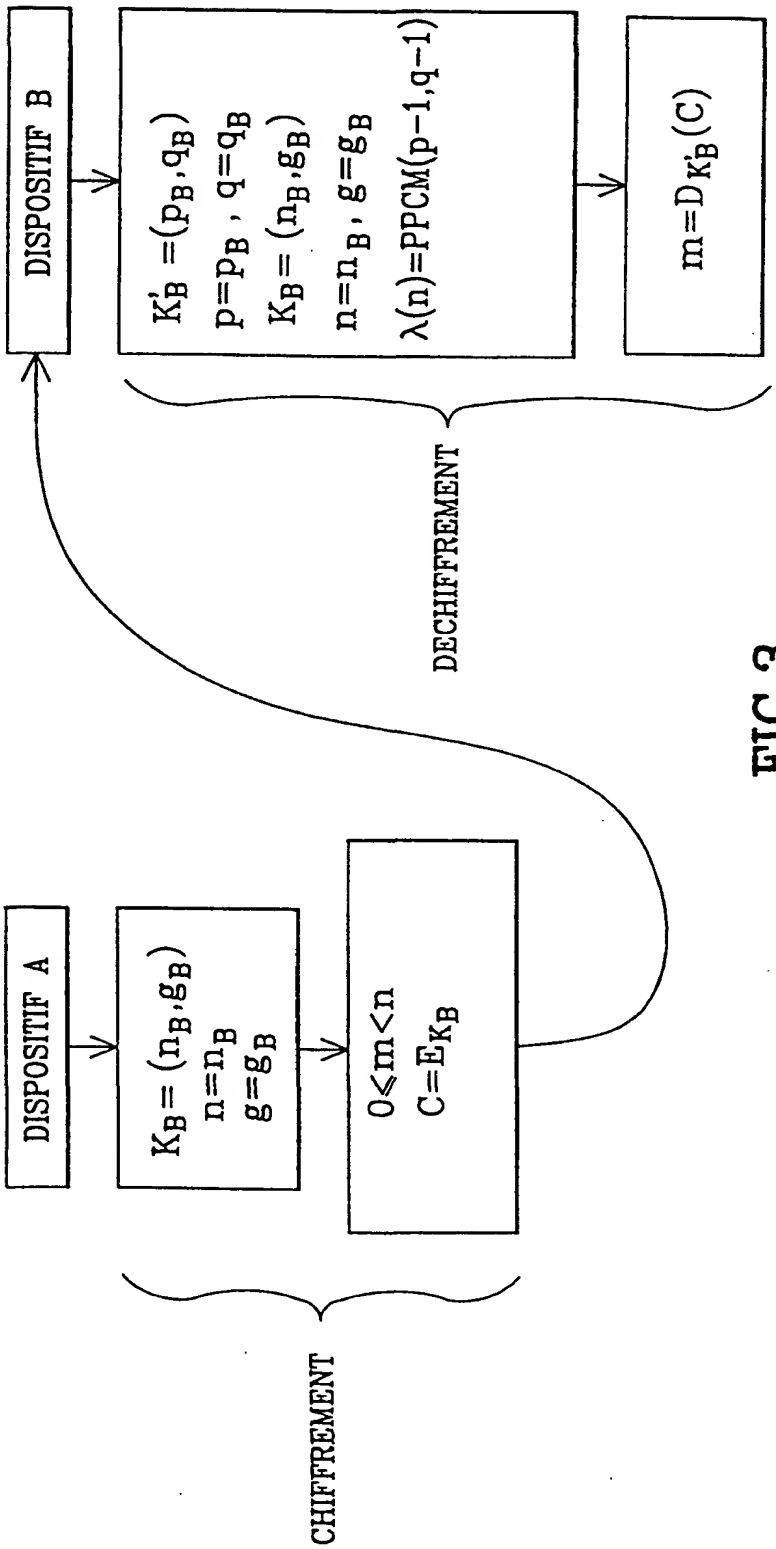

DISPOSITIF A
$K_B = (n_B, g_B)$
$n = n_B$
$g = g_B$
$0 \leqslant m < n$
$C = E_{K_B}$
CHIFFREMENT
DISPOSITIF B
$K'_B = (p_B, q_B)$
$p = p_B$, $q = q_B$
$K_B = (n_B, g_B)$
$n = n_B$, $g = g_B$
$\lambda(n) = PPCM(p-1, q-1)$
$m = D_{K'_B}(C)$
DECHIFFREMENT

FIG.3

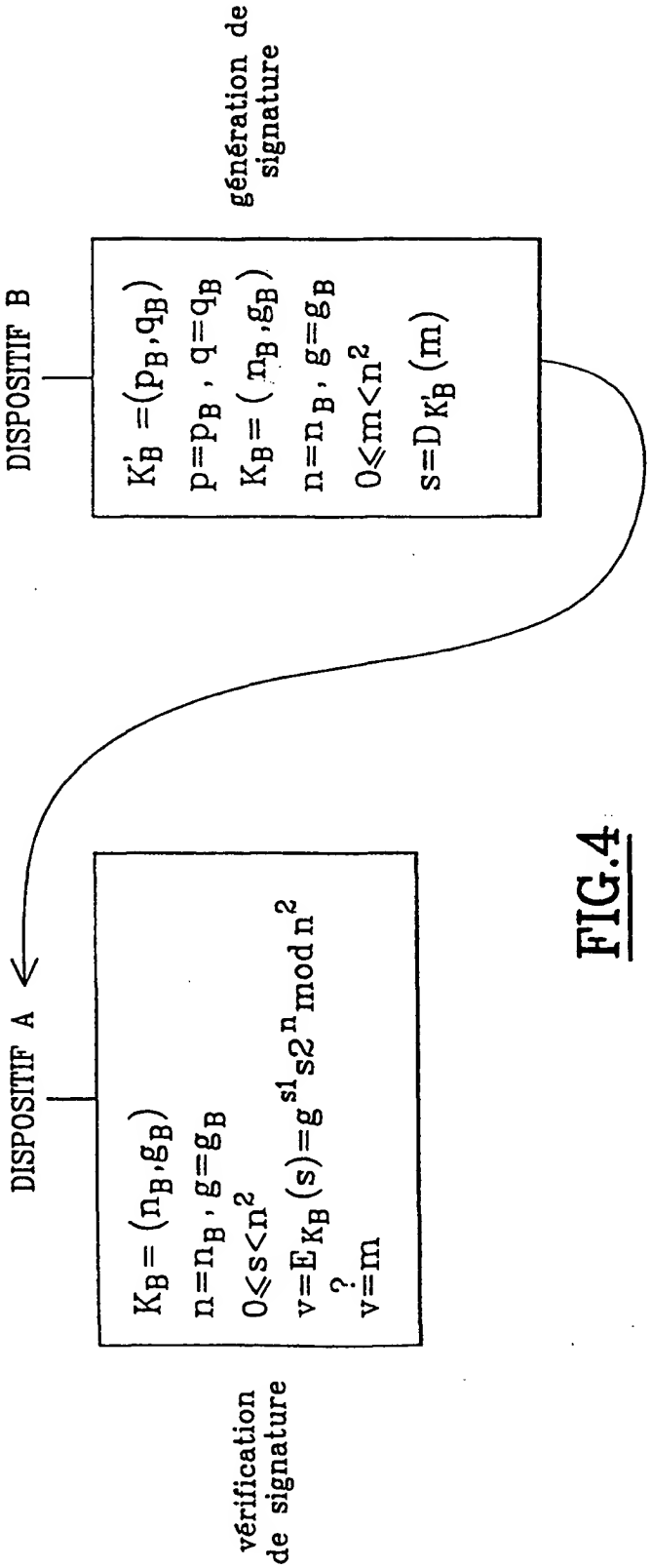

DISPOSITIF B
génération de signature
$K'_B = (p_B, q_B)$
$p = p_B$, $q = q_B$
$K_B = (n_B, g_B)$
$n = n_B$, $g = g_B$
$0 \leqslant m < n^2$
$s = D_{K'_B}(m)$
DISPOSITIF A
vérification de signature
$K_B = (n_B, g_B)$
$n = n_B$, $g = g_B$
$0 \leqslant s < n^2$
$v = E_{K_B}(s) = g^{s1} s2^n \bmod n^2$
?
$v = m$

FIG.4

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/FR 99/02918

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YASUKO GOTOH ET AL: "A METHOD FOR RAPID RSA KEY GENERATION" SYSTEMS & COMPUTERS IN JAPAN, vol. 21, no. 8, 1 January 1990 (1990-01-01), pages 11-20, XP000177817 ISSN: 0882-1666 page 12, right-hand column, line 12 -page 13, left-hand column, line 12	1,16

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 2000	18/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

De[illegible]le internationale No
PCT/FR 99/02918

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	YASUKO GOTOH ET AL: "A METHOD FOR RAPID RSA KEY GENERATION" SYSTEMS & COMPUTERS IN JAPAN, vol. 21, no. 8, 1 janvier 1990 (1990-01-01), pages 11-20, XP000177817 ISSN: 0882-1666 page 12, colonne de droite, ligne 12 -page 13, colonne de gauche, ligne 12	1,16

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 février 2000	18/02/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

1

Translation 09/889352

6

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GEM 603	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/02918	International filing date (*day/month/year*) 25 November 1999 (25.11.99)	Priority date (*day/month/year*) 14 January 1999 (14.01.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/30		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 29 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12 July 2000 (12.07.00)	11 April 2001 (11.04.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/02918

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages _____, as originally filed,
pages _____, filed with the demand,
pages 1-21, filed with the letter of 02 March 2001 (02.03.2001),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-20, filed with the letter of 02 March 2001 (02.03.2001),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 2/4-4/4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig 1/4, filed with the letter of 02 March 2001 (02.03.2001),
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-20	YES
	Claims		NO
Inventive step (IS)	Claims	1-20	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-20	YES
	Claims		NO

2. Citations and explanations

The following document is referred to:

D1: YASUKO GOTOH ET AL.: "A method for rapid rsa key generation", Systems & Computers in Japan, Vol. 21, N° 8, 1 January 1990, pages 11-20, XP000177817, ISSN: 0882-1666.

1. Independent Claim 1 concerns an asymmetrical cryptographic method with public and private keys.

According to the current prior art, the RSA method alone can be used either for message encryption or for generating a digital signature. However, the calculation time in this method is often very long.

The present invention therefore provides an asymmetrical cryptographic method (private key and public key), which enables messages to be encrypted and signed and which, in certain configurations, has a more rapid processing time than an RSA method. The method uses an encryption and decryption algorithm which makes use of a property of the logarithms (described in detail on page 7 of the

description).

D1, which is considered to be closest, discloses a method for rapidly generating public and private keys in an RSA method. The solution for selecting the numbers p and q (private key) is not only rapid (the private key can be generated at the user end itself) but also protected against factoring attacks.

However, D1 does not disclose the same cryptogram. The cryptogram disclosed in Claim 1 is: $c = g^m \bmod n$, whereas the cryptogram used in D1 is: $c = m^e \pmod n$. The number m representing the message is used as the exponent in Claim 1, rather than as the base of a power below the exponent.

With this solution, particularly where g=2, the calculation of the power is simplified and a faster algorithm processing time is achieved.

This solution is neither known nor derivable from D1, and the subject matter of Claim 1 is therefore considered to be novel (PCT Article 33(2)) and to involve an inventive step (PCT Article 33(3)).

2.1 Independent Claim 2 concerns the use of the method presented in Claim 1 in a system for communication between a first device and a second device, and its subject matter is therefore likewise considered to be novel (PCT Article 33(2)) and inventive (PCT Article 33(3)).

2.2 Claims 3-7 are dependent on Claim 2 and therefore likewise satisfy the PCT requirements of novelty and inventive step.

THIS PAGE BLANK (USPTO)

3.1 Independent Claim 9 concerns the use of the method presented in Claim 1 in a system for communication between a first device and a second device with the additional feature that the number m representing the message is used to calculate the two numbers m1 and m2, which provides the method with the additional property that it can also be used for signature; its subject matter is therefore considered to be novel (PCT Article 33(2)) and to involve an inventive step PCT Article 33(3)).

3.2 Claims 10-14 are dependent on Claim 9 and therefore likewise satisfy the PCT requirements of novelty and inventive step.

4.1 Claims 15 and 16 are identical to Claims 2 and 3 and their subject matter is therefore likewise considered to be novel (PCT Article 33(2)) and to involve an inventive step (PCT Article 33(3)).

4.2 Claims 17-20 are dependent on Claim 15 and therefore likewise satisfy the PCT requirements of novelty and inventive step.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. In order to satisfy the requirements of PCT Rule 6.3(b), the independent claims should be drafted **correctly** in two parts, with features known in combination from prior art (see D1) being mentioned in the first part.

2. In order to satisfy the requirements of PCT Rule 11.13(l), reference signs 1 and 2, which are mentioned in the description on page 7, lines 19 and 24, must appear in at least one of the drawings, failing which they should not appear in the description.

3. The applicant must correct the following mistakes in the description:

(i) page 13, line 22:

$$\log_p(x) = \frac{x-1}{p}$$

(ii) page 13, line 22:

$$\log_q(x) = \frac{x-1}{q}$$

(iii) Claim 5:

$$\log_q(x) = \frac{x-1}{n}$$

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. According to the PCT there are in fact only two basic types of claim, namely claims to a physical entity (device) and claims to an activity (process) (see PCT Examination Guidelines, Chapter III-3.1). Consequently, a device claim should contain only structural features (means to...), and not functional features.

On this issue, some of the expressions used, such as:
"system... with keys... generated **in accordance with Claim 1" (Claims 2, 9 and 15);**
"system... characterised in that an encryption method is used..." **(Claims 2, 9 and 15);**
"the device: carries out... calculates.." (the set of claims);
"Process as per Claim 17" (claim to a system)
can not be considered as defining either structural features or activities (functions), and they are therefore not clearly categorised either as device claims or as process claims.

The clarity of the claims is extremely important, given their role in defining the subject matter for which protection is sought. In view of the different extents of protection that may be granted to the various categories of claim, the text must leave no doubt as to the category to which a claim belongs (PCT Article 6, and PCT Examination Guidelines, Chapter III-4.1).

VIII. Certain observations on the international application

The applicant should therefore preferably have drafted all of the claims as process claims.

2. The subject matter of Claims 15 and 16 merely repeats Claims 2 and 3, respectively, and as a result, contrary to PCT Article 6, the two claims are not concise.

3. Contrary to PCT Article 6, the subject matter of Claim 1 is not clearly defined for the following reason: the parameter "m" is not defined in the claims before it is used in the corresponding mathematical formula.

09/889362

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 603	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02918	Date du dépot international *(jour/mois/année)* 25/11/1999	Date de priorité *(jour/mois/année)* 14/01/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/30		
Déposant GEMPLUS S.C.A. et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 8 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 23 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
12/07/2000	11.04.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Grimaldo, M N° de téléphone +49 89 2399 7513

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02918

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-21	reçue(s) le	02/03/2001	avec la lettre du	26/02/2001

Revendications, N°:

1-20	reçue(s) le	02/03/2001	avec la lettre du	26/02/2001

Dessins, feuilles:

2/4-4/4	version initiale			
1/4	reçue(s) le	02/03/2001	avec la lettre du	26/02/2001

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :
   ☐ des revendications, n^{os} :
   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-20
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-20
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-20
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Documents mentionnés

Il est fait référence au document suivant:

D1: YASUKO GOTOH ET AL.: "A method for rapid rsa key generation", Systems & Computers in Japan, vol. 21, no. 8, 1 Janvier 1990, pages 11-20, XP000177817, ISSN: 0882-1666

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. La revendication indépendante 1 concerne un procédé cryptographique asymétrique à clés publique et privée.

Selon l'état actuel de la technique, seul le procédé RSA peut être utilisé soit pour le chiffrement des messages soit pour la génération de signature numérique. Toutefois, le temps de calcul de cette procédure est souvent très long.

L'invention propose donc un procédé cryptographique asymétrique (clé secrète et clé publique) qui permet de chiffrer des messages et aussi de les signer et qui, dans certaines configurations, a un temps de traitement plus rapide qu'un procédé RSA.
Le procédé utilise un l'algorithme de cryptage et decryptage qui tire avantage d'une propriété des logarithmes (décrit en détails à la page 7 de la description).

Le document D1, considéré comme le plus proche, dévoile un méthode rapide pour générer des clés publique et privée dans un procédé RSA. La solution pour choisir le nombres p et q (clé privée) est, à la fois, rapide (la clé privée peut être crée dans l'utilisateur même) et sécurisée contre un attaque de factorisation.

Cependant, le document D1 ne dévoile pas le même cryptogramme.
Le cryptogramme divulgué par la revendication 1 est: $c = g^m \bmod n^2$, tandis que le cryptogramme utilisé dans le document D1 est: $c = m^e \pmod n$: le nombre m

THIS PAGE BLANK (USPTO)

représentatif du message est utilisé comme exposant dans la revendication 1 tandis que sous l'exposant en tant que base d'une puissance.

Dans cette solution, en particulier si g=2, le calcul de la puissance est facilité et le temps de traitement de l'algorithme est plus rapide.

Cette solution n'est ni connue, ni dérivable, du document D1 et, donc, l'objet de la revendication 1 est considéré comme nouveau (Article 33(2) PCT) et impliquant une activité inventive (Article 33(3) PCT).

2.1 La revendication indépendante 2 considère l'utilisation du procédé présenté dans la revendication 1 dans une système de communication entre un premier et un deuxième dispositif et donc, son objet est considéré comme nouveau (Article 33(2) PCT) et inventif aussi (Article 33(3) PCT).

2.2 Les revendications 3-7 dépendent de la revendication 2 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

3.1 La revendication indépendante 9 considère l'utilisation du procédé présenté dans la revendication 1 dans une système de communication entre un premier et un deuxième dispositif en ajoutant la caractéristique que le nombre m représentatif du message est utilisé pour calculer les deux nombre m1 et m2 qui confère au procédé la propriété supplémentaire de pouvoir être utilisé aussi en signature et donc, son objet est considéré comme nouveau (Article 33(2) PCT) et impliquant une activité inventive (Article 33(3) PCT).

3.2 Les revendications 10-14 dépendent de la revendication 9 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

4.1 Les revendication 15 et 16 sont identiques aux revendications 2 et 3 et donc, leur objet est considéré comme nouveau (Article 33(2) PCT) et impliquant une activité inventive aussi (Article 33(3) PCT).

4.2 Les revendications 17-20 dépendent de la revendication 15 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

VII. Irrégularités dans la demande internationale

1. En vue de remplir les conditions de la Règle 6.3(b) PCT, les revendications indépendantes devraient être **correctement** présentées en deux parties, les caractéristiques qui, combinées, sont comprises dans l'état de la technique (voir document D1) étant indiquées dans la première partie.

2. En vue de remplir les conditions énoncées à la Règle 11.13(l), les signes de référence 1 et 2 mentionnés dans la description à la page 7, lignes 19 et 24 doivent apparaître au moins dans un des dessins ou ne doivent pas apparaître dans la description.

3. Le Demandeur devra corriger les erreurs suivantes dans la description:
   i) à la page 13, ligne 22:

$$\log_p(x)=\frac{x-1}{p}$$

   ii) à la page 13, ligne 22:

$$\log_q(x)=\frac{x-1}{q}$$

   iiii) revendication 5:

$$\log_n(x)=\frac{x-1}{n}$$

VIII. Observations relatives à la demande internationale

1. Selon le PCT il n'existe en réalité que deux types fondamentaux de revendications, à savoir les revendications portant sur une entité physique (dispositif) et les revendications portant sur une activité (procédé) (Cf. Directives PCT C-III, 3.1).
Par conséquent, une revendication de dispositif ne devrait contenir que des caractéristiques structurelles (moyens pour...) et non des caractéristiques fonctionnelles.

   A ce propos, des formulations utilisées, par exemple, comme:
"système .. à clés ... générées **selon la revendication 1" (revendications 2, 9 et 15);**
"système... caractérisé en ce que un procédé de chiffrement est mis en oeuvre..." **(revendications 2, 9 et 15);;**
"le dispositif: effectue... calcule..." (jeux de revendications);
"Procédé selon la revendication 17 (revendication de système)
ne peuvent pas être considérées comme définissant ni des caractéristiques structurelles ni des activités (fonction) et donc ne sont pas clairement ni revendication d'appareil ni revendication de procédé.

   La clarté des revendications est d'une extrême importance, étant donné le rôle qu'elles jouent dans la définition de la matière pour laquelle la protection est demandée. En raison des différences d'étendue de la protection que l'on peut attribuer aux diverses catégories de revendications, le texte d'une revendication ne doit laisser subsister aucun doute quant à la catégorie à laquelle elle appartient (Article 6 du PCT et Directives PCT C-III, 4.1).

   A cet égard, le Demandeur aurait dû de préférence présenter tous les revendications sous la forme de revendications de procédé.

2. L'objet des revendications 15 et 16 n'est qu'une répétition des revendications 2 et 3 respectivement et les deux revendications ne sont pas concise comme l'exige l'Article 6 PCT.

3. L'objet de la revendication 1 n'est pas clairement défini comme l'exige l'Article 6 PCT pour la raison suivante: le paramètre "m" n'a pas été défini dans les revendications avant de l'utiliser dans l'expression mathématique associée.

PROCEDE CRYPTOGRAPHIQUE A CLES PUBLIQUE ET PRIVEE

La présente invention concerne un procédé cryptographique à clés publique et privée. Il est utilisable dans toutes les applications dans lesquelles il est nécessaire d'assurer la confidentialité des messages transmis sur un canal quelconque et/ou d'identifier avec certitude un dispositif avec lequel on échange des messages.

La confidentialité de messages transmis entre deux dispositifs A et B sur un canal de communication quelconque est obtenue en chiffrant l'information transmise pour la rendre inintelligible aux personnes à qui elle n'est pas destinée. L'identification certaine d'un dispositif est lui basé le calcul de la signature numérique d'un message.

En pratique, deux types de procédé cryptographique peuvent être utilisés celui dit symétrique, à clés secrètes, dont un exemple bien connu est le DES...celui dit asymétrique, utilisant une paire de clés publique et privée et décrit dans " *Public_key cryptosystem* " *dans* " *New directions in Cryptographie* " *IEEE Transactions on Information Theory, nov. 1976, par* MM Diffie et Hellman. Un exemple bien connu de procédé asymétrique est le RSA, du nom de ses inventeurs Ronald Rivest, Adi Shamir et Léonard Adleman. On peut trouver une description de ce procédé RSA dans le brevet américain US 4, 405, 829.

Dans l'invention, on s'intéresse plus particulièrement à un procédé cryptographique asymétrique.

Un procédé de chiffrement selon un procédé cryptographique asymétrique consiste principalement, pour un émetteur A qui veut envoyer confidentiellement un message à un destinataire B à prendre connaissance, par

exemple dans un annuaire, de la clé publique K_B du destinataire B, à appliquer dans le procédé de chiffrement E sur le message m à transmettre, et à envoyer au destinataire B, le cryptogramme c résultant :

$$c = E_{K_B}(m).$$

Ce procédé consiste principalement pour le destinataire B, à recevoir le cryptogramme c, et à le déchiffrer pour obtenir le message d'origine m, en appliquant la clé privée K'b qu'il est le seul à connaître dans le procédé de déchiffrement D sur le cryptogramme c : $m = D_{K'_B}(c)$.

Selon ce procédé n'importe qui peut envoyer un message chiffré au destinataire B, mais seul ce dernier est capable de le déchiffrer.

On utilise habituellement un procédé cryptographique asymétrique pour la génération/vérification de signature. Dans ce contexte, un utilisateur qui veut prouver son identité utilise une clé privée, connue de lui seul, pour produire une signature numérique s d'un message m, signature qu'il transmet au dispositif destinataire. Ce dernier met en oeuvre la vérification de la signature en utilisant la clé publique de l'utilisateur. Tout dispositif a ainsi la capacité de vérifier la signature d'un utilisateur, en prenant connaissance de la clé publique de cet utilisateur et en l'appliquant dans l'algorithme de vérification. Mais seul l'utilisateur concerné a la capacité de générer la bonne signature utilisant sa clé privée. Ce procédé est par exemple beaucoup utilisé dans les systèmes de contrôle d'accès ou de transactions bancaires. Il est en général couplé à l'utilisation d'un procédé de chiffrement, pour chiffrer la signature avant de la transmettre.

Pour cette génération/vérification de signatures numériques, on peut utiliser en pratique des procédés cryptographiques asymétriques dédiés à cette application,

tel le DSA *(Digital Signature Algorithm)*, qui correspond à un standard américain proposé par le *US National Institute of Standards and Technology*. On peut en outre utiliser le RSA qui a la propriété de pouvoir être utilisé aussi bien en chiffrement qu'en génération de signature.

Dans l'invention, on s'intéresse à un procédé cryptographique qui puisse être utilisé pour le chiffrement des messages et pour la génération de signature numérique. Dans l'état actuel de la technique, seul le RSA, dont il existe de nombreuses variantes de mise en oeuvre, offre cette double fonctionnalité.

Le RSA comprend une étape de génération des clés publique K et privée K' pour un dispositif donné dans laquelle on procède de la façon suivante :

- on choisit deux grands nombres premiers p et q, distincts.

- on calcule leur produit n=p.q.

- on choisit un nombre e premier avec le plus petit commun multiple de (p-1)(q-1). En pratique, e est souvent pris égal à 3.

La clé publique K est alors formée par le couple de paramètres (n,e) et la clé secrète K' est formée par le couple de paramètres (p,q).

En choisissant p et q de grande taille, leur produit n est aussi de grande taille. n est donc très difficile à factoriser : on est assuré que l'on ne pourra pas retrouver la clé secrète K'=(p,q) à partir de la connaissance de n .

Le procédé de chiffrement d'un nombre m représentant un message M, $0 \leq m < n$ consiste alors, à effectuer le calcul suivant :

$c = E_B(m) = m^e \bmod n$

au moyen de la clé publique K=(n,e).

Le procédé de déchiffrement consiste lui dans le calcul inverse suivant :

$m=c^d \bmod(n)$

au moyen de la clé privée K'=(p,q), gardée secrète, où

$$d=\frac{1}{e} \bmod (p-1)(q-1).$$

On a vu que le RSA a la particularité d'être utilisable pour la vérification de signature. Le procédé correspondant de génération de signature par un utilisateur A consiste à utiliser le procédé de déchiffrement avec la clé secrète pour produire la signature s d'un nombre m représentatif d'un message. On a ainsi : $s=m^d \bmod n$.

Cette signature s est transmise à un destinataire B.Ce dernier, qui connaît m (par exemple, A transmet s et m), vérifie la signature en effectuant l'opération inverse, c'est à dire en utilisant le procédé de chiffrement avec la clé publique de l'émetteur A. C'est à dire qu'il calcule $v=s^e \bmod n$, et vérifie v=m.

En général, pour améliorer la sécurité d'un tel procédé de vérification de signature, on applique préalablement une fonction de hachage sur le nombre m avant de calculer la signature, qui peut consister en des permutations de bits et/ou une compression.

Quand on parle de message M à chiffrer ou à signer, il s'agit bien sûr de messages numériques, qui peuvent résulter d'un codage numérique préalable. Ce sont en pratique des chaînes de bits, dont la taille binaire (nombre de bits) peut être variable.

Or un procédé de cryptographie comme le RSA est tel qu'il permet de chiffrer avec la clé publique (n,e) n'importe quel nombre entre 0 et n-1. Pour l'appliquer à un message M de taille quelconque, il faut donc en pratique couper ce message en une suite de nombres m qui vérifieront chacun la condition $0 \leq m < n$. On applique alors

le procédé de chiffrement sur chacun de ces nombres. Dans la suite, on s'intéresse donc à l'application du procédé cryptographique sur un nombre m représentatif du message M. m peut-être égal à M, ou en n'être qu'une partie. On désigne alors indifféremment dans la suite par m le message ou un nombre représentatif du message.

Un objet de l'invention, est un procédé de cryptographie asymétrique différent de ceux basés sur le RSA.

Un objet de l'invention, est un procédé reposant sur d'autres propriétés, qui puisse s'appliquer aussi bien en chiffrement de messages qu'en génération de signatures.

Un objet de l'invention, est un procédé de cryptographique qui permette, dans certaines configurations, un temps de traitement plus rapide.

Telle que caractérisée, l'invention concerne un procédé cryptographique selon la revendication 1.

L'invention sera mieux comprise à la lecture de la description suivante , faite à titre indicatif et nullement limitatif de l'invention et en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma fonctionnel d'un système de communication cryptographique de type asymétrique;
- la figure 2 est un schéma fonctionnel d'un dispositif communiquant utilisé dans un système de communication cryptographique selon l'invention;
- la figure 3 est un organigramme d'une session de chiffrement/déchiffrement de messages utilisant le procédé cryptographique selon l'invention; et
- la figure 4 est un organigramme d'une session de génération/vérification de signature utilisant le procédé cryptographique selon l'invention.

Pour bien comprendre l'invention, il est nécessaire de faire quelques préliminaires mathématiques.

Dans la description, on utilise les notations mathématiques suivantes :

(1) Si a est un entier relatif et b un entier strictement positif, a mod b (a modulo b) est le résidu modulaire de a relativement à b et désigne l'unique entier strictement inférieur à b tel que b divise (a - a mod b).

(2) (Z/bZ) désigne l'ensemble des résidus modulo b et forme un groupe pour l'addition modulaire .

(3) $(Z/bZ)^*$ désigne l'ensemble des entiers inversibles modulo b et forme un groupe pour la multiplication modulaire.

(4) L'ordre d'un élément a de $(Z/bZ)^*$ est le plus petit entier naturel ord(a,b) tel que $a^{ord(a,b)}=1 \bmod b$.

(5) PPCM (a,b) désigne le plus petit commun multiple de a et b.

(6)PGCD(a,b) désigne le plus grand commun diviseur de a et b.

(7) $\lambda(a)$ désigne l'indicateur d'Euler de a. Si a=p.q, $\lambda(a)$=PPCM(p-1,q-1).

(8) On note $x=TRC(a_1,...a_k, b_1,...b_k)$ l'unique solution, obtenue par la mise en oeuvre du Théorème du Reste Chinois bien connu, du système d'équations modulaires suivant :

$x=a_1 \bmod b_1$

$x= a_2 \bmod b_2$

...

$x= a_k \bmod b_k$.

où les entiers a_i et b_i sont donnés et où, $\forall i,j$ avec $i \neq j$, PGCD(b_i, b_j)=1.

(9) On rappelle que la taille binaire d'un nombre a est le nombre de bits sur lesquels a s'écrit.

Soit maintenant un nombre n, entier, de taille arbitraire. L'ensemble $Un=\{x<n^2 / x=1 \bmod n\}$ est un sous-groupe multiplicatif de $(Z/n^2Z)^*$.

Soit alors $\log_n$ la fonction définie sur l'ensemble Un par :

$$\log_n(x)= \frac{x-1}{n}$$

Cette fonction a la propriété suivante :

$\forall x \in Un, \forall y \in Un, \log_n(xy \bmod n^2)= \log_n(x) + \log_n(y) \bmod n$.

Par conséquent, si g est un nombre entier arbitraire appartenant à Un, on a pour tout nombre m, $0 \leq m < n$:

$\log_n(g^m \bmod n^2)=m.\log_n(g) \bmod n^2$.

Cette propriété mathématique est à la base du procédé de cryptographie mis en oeuvre dans l'invention qui va maintenant être décrite.

La figure 1 représente un système de communication cryptographique, utilisant un procédé cryptographique asymétrique. Il comprend des dispositifs communiquants, dans l'exemple A et B, sur un canal de communication 1. Dans l'exemple, on a représenté un canal bidirectionnel. Chaque dispositif contient une paire de clés publique K et privée K'.

Les clés publiques sont par exemple publiées dans un fichier public 2 tel qu'un annuaire, que chaque dispositif peut consulter. Dans ce fichier public, on trouvera ainsi la clé publique K_A du dispositif A et celle K_B du dispositif B.

La clé privée K' de chaque dispositif est conservée par lui de façon secrète, typiquement dans une zone sécurisée de mémoire non volatile. Le dispositif A contient ainsi en mémoire secrète sa clé privée K'_A et le dispositif B contient ainsi en mémoire secrète sa clé

privée K'_B. Ils conservent aussi leur clé publique, mais dans une zone mémoire sans protection d'accès particulière.

Dans un tel système, le dispositif A peut chiffrer un message m en un cryptogramme c_A en utilisant la clé publique K_B du dispositif B; ce dernier peut déchiffrer c_A en utilisant sa clé privée K'_B, qu'il conserve secrètement. Inversement, le dispositif B peut chiffrer un message m en un cryptogramme c_B en utilisant la clé publique K_A du dispositif A; ce dernier peut déchiffrer c_B en utilisant sa clé privée K'_A, qu'il conserve secrètement.

Typiquement, chaque dispositif comprend au moins, comme représenté sur la figure 2, des moyens de traitement 10, c'est à dire une unité centrale de traitement (CPU), comprenant notamment différents registres R pour le calcul, une interface de communication 11 avec le canal de communication, et des moyens de mémorisation. Ces moyens de mémorisation comprennent généralement une mémoire programme 12 (ROM, EPROM, EEPROM) et une mémoire de travail (RAM) 13 . En pratique, chaque dispositif conserve ses données secrètes dans une zone d'accès sécurisée 120 prévue en mémoire programme et ses données publiques dans une zone d'accès normal de cette mémoire. La mémoire de travail permet de conserver momentanément, le temps nécessaire aux calculs, des messages à chiffrer, des cryptogrammes à déchiffrer, ou encore des résultats de calculs intermédiaires.

Les moyens de traitement et de mémorisation permettent ainsi d'exécuter des programmes liés à l'application, et notamment d'effectuer les calculs correspondant à la mise en oeuvre du procédé de cryptographie pour le chiffrement /déchiffrement de messages et/ou la génération/vérification de signatures. selon l'invention. Ces calculs comprennent notamment,

comme on le verra de façon détaillée dans la suite, des élévations à la puissance, des résidus et inversions modulaires .

Les dispositifs peuvent encore comprendre un générateur 14 de nombre aléatoire ou pseudo-aléatoire r , qui peut intervenir dans les calculs précités, dans certaines variantes de réalisation. Ce générateur est encadré en pointillé sur la figure 2, pour indiquer qu'il n'est pas nécessaire à la réalisation de toutes les variantes de réalisation selon l'invention.

Tous ces moyens du dispositif sont connectés à un bus d'adresses et de données 15.

De tels dispositifs utilisés dans l'invention sont bien connus, et correspondent par exemple à ceux qui sont utilisés dans les systèmes de communication cryptographique de l'état de la technique, mettant en oeuvre le RSA. Ils ne seront donc pas détaillés plus avant. Un exemple pratique de système de communication cryptographique, est le système formé des serveurs bancaires et des cartes à puce, pour la gestion de transactions financières. Mais il existe de nombreuses autres applications, telle les applications liées au commerce électronique .

Un premier mode de réalisation de l'invention va maintenant être détaillé, au regard de l'organigramme représenté sur la figure 3.

Cet organigramme représente une séquence de communication entre un dispositif A et un dispositif B sur un canal de communication 20. Ces dispositifs comprennent au moins les moyens de traitement, de mémorisation et de communication décrits en relation avec la figure 2.

Le procédé de cryptographie selon l'invention comprend un procédé de générations des clés publique K et privée K'.

Selon l'invention, ce procédé de génération des clés publique et privée d'un dispositif comprend les étapes suivantes qui sont déjà connues dans le document de YASUKO GOTOH et al publié en Janvier 1990 au JAPON, sous les références XP000177817, ISSN : 0882-1666, vol. 21 n° 8 – pages 11-20 de « a method for rapid RSA Key generation » de l'ouvrage « Systems & Computers »:

- sélection de deux grands nombres premiers p et q distincts et de taille voisine;
- calcul du nombre n égal au produit p.q;
- calcul du nombre $\lambda(n)=PPCM(p-1, q-1)$, c'est à dire de la fonction de Carmichael du nombre n;
- détermination d'un nombre g, $0 \leq g < n^2$, qui remplisse les deux conditions suivantes :

a) g est inversible modulo n^2 et

b) $ord(g,n^2)=1 \bmod n$.

Cette condition b) indique que l'ordre du nombre g dans l'ensemble $(Z/n^2Z)^*$ des nombres entiers de 0 à n^2 est un multiple non nul du nombre n, selon les notations définies plus haut.

La clé publique K est alors formée par le nombre n et le nombre g. La clé privée est formée par les nombres p,q et $\lambda(n)$ ou seulement par les nombres p et q, $\lambda(n)$ pouvant être recalculé à chaque utilisation de la clé secrète.

On génère selon ce procédé les clés publique et privée de chaque dispositif. Cette génération peut-être effectuée, selon les dispositifs considérés et les applications, par les dispositifs eux-mêmes ou par un organe externe.

Chaque dispositif, par exemple le dispositif A, contient donc en mémoire sa clé publique $K_A = (n_A, g_A)$ et, de façon secrète, sa clé privée $K'_A = (p_A, q_A)$.

En outre, les clés publiques sont mises dans un fichier accessible au public.

Selon l'invention, on verra ci-dessous qu'elle consiste à donner une valeur particulière à g. En effet, il est avantageux de choisir g=2, lorsque c'est possible, c'est à dire, lorsque g=2 remplit les conditions a) et b) du procédé de génération de signature selon l'invention.

Un procédé de chiffrement selon un premier mode de réalisation du procédé cryptographique de l'invention mis en oeuvre dans le dispositif A consiste alors, pour l'envoi d'un message au dispositif B, dans la réalisation des étapes suivantes, avec $0 \leq m < n$:

- renseignement des paramètres n et g du procédé de chiffrement mis en oeuvre par le dispositif A par la clé publique K_B du deuxième dispositif B : $n = n_B$, $g = g_B$.
- calcul du cryptogramme $c = g^m \bmod n^2$, et
- transmission du cryptogramme c sur le canal de communication.

Le procédé de chiffrement selon un premier mode de réalisation de l'invention consiste donc à prendre le paramètre g de la clé publique, à l'élever à la puissance m, et à calculer le résidu modulaire relativement à n^2. On notera que dans le RSA, c'est le message m qui est élevé à la puissance alors que dans l'invention, le message m est utilisé comme exposant.

Le dispositif B qui reçoit le message chiffré, c'est à dire le cryptogramme c, met alors en oeuvre un procédé de déchiffrement selon l'invention avec les paramètres de sa clé privée. Ce procédé de déchiffrement comprend le calcul suivant :

- calcul du nombre m tel que

$$m = \frac{\log_n(c^{\lambda(n)} \bmod n^2)}{\log_n(g^{\lambda(n)} \bmod n^2)} \bmod n$$

où

$$\log_n(x) = \frac{x-1}{n}$$

Si g=2, on voit que le calcul d'élévation de g à la puissance est facilité. On prendra donc de préférence g=2, toutes les fois où ce sera possible. En d'autres termes, le procédé de génération des clés commencera par essayer si g=2 remplit les conditions a) et b).

Différentes variantes de calcul du procédé de déchiffrement peuvent être mises en oeuvre, qui permettent, lorsque le dispositif doit déchiffrer un grand nombre de cryptogrammes, de précalculer certaines quantités et de les conserver de façon secrète dans le dispositif. Une contrepartie est que la zone mémoire secrète (zone 120 sur la figure 2) du dispositif doit être plus étendue, puisqu'elle doit alors contenir alors des paramètres supplémentaires en plus des paramètres p et q. Ceci n'est pas sans influencer le choix de mise en eouvre d'une variante ou d'une autre. En effet, la réalisation d'une zone de mémoire sécurisée est coûteuse, et donc de capacité (mémoire) généralement limitée, notamment dans les dispositifs dits à bas côuts (par exemple, certains types de cartes à puce).

Dans une première variante de mise en oeuvre du procédé de déchiffrement, on prévoit que le dispositif, B

en l'occurrence, précalcule une fois pour toutes la quantité :

$$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

et la conserve secrète en mémoire.

Ainsi, on réduit d'autant le temps nécessaire au déchiffrement de chacun des messages reçus par le dispositif. En effet, lorsque que le dispositif B exécute une instance de cette variante du procédé de déchiffrement, il ne lui reste plus qu'à calculer :

$$m = \log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n.$$

Dans une deuxième variante de mise en oeuvre du procédé de déchiffrement selon l'invention, on prévoit d'utiliser le Théorème du Reste Chinois, pour une meilleure efficacité (rapidité du calcul).

Dans une instance de cette deuxième variante du procédé de déchiffrement, le dispositif effectue les calculs (de déchiffrement) suivants :

1 $m_p = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

2 $m_q = \log_q(c^{q-1} \bmod q^2)\log_p(g^{q-1} \bmod q^2)^{-1} \bmod q$

3 $m = TRC(m_p, m_q, p, q)$, où

$$\log_p(x) \quad \frac{x-1}{p} \quad \text{et}$$

$$\log_q(x) \quad \frac{x-1}{q}$$

Dans ce cas, on peut en outre prévoir, dans les cas où le dispositif est amené à déchiffrer un très grand nombre de messages, que le dispositif précalcule une fois pour toutes les quantités suivantes :

$$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p \text{ et}$$

$$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$$

Le dispositif doit alors conserver ces quantités comme données secrètes.

Le calcul effectué lors d'une instance du procédé de déchiffrement devient :

1. $m_p=\log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $m_q=\log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
3. $m=TRC(m_p,m_q,p,q)$.

Comme déjà précisé, toutes ses variantes de calcul de déchiffrement sont intéressantes lorsque le dispositif est amené à déchiffrer un très grand nombre de messages, et que le gain en temps de traitement compense la plus grande capacité mémoire de la zone sécurisée pour conserver toutes les données secrètes. Le choix de l'une ou l'autre variante dépend en pratique de l'application considérée et des contraintes de coûts et de temps de traitement à concilier.

Un deuxième mode de réalisation de l'invention comprend l'utilisation d'un nombre aléatoire, fournit par un générateur de nombre aléatoire (ou pseudo-aléatoire), dans le procédé de chiffrement, en sorte que pour un même message m à transmettre, le cryptogramme calculé c sera différent à chaque fois. La sécurité du système de communication est donc plus grande. Le procédé de déchiffrement est inchangé.

Ce deuxième mode de réalisation de l'invention comprend deux variantes.

Dans une première variante, le cryptogramme c est obtenu par le calcul suivant : $c=g^{m+nr} \bmod n^2$.

Dans une deuxième variante, le cryptogramme c est obtenu par le calcul suivant : $c=g^m r^n \bmod n^2$.

Cette deuxième variante nécessite en pratique un temps de traitement plus long que la première, mais elle offre une plus grande sécurité.

Dans un troisième mode de réalisation de l'invention, on impose que l'ordre de g dans $(Z/nZ)^*$ soit un entier de petite taille, ceci étant obtenu par une mise en oeuvre du procédé de génération des clés différente.

Avec une telle condition sur l'ordre du paramètre g, on réduit la complexité du calcul du procédé de déchiffrement qui devient en pratique quadratique (fonction de n^2) par rapport à la taille du nombre n.

Dans ce troisième mode de réalisation de l'invention, le procédé de génération des clés publique et privée est alors le suivant :

- sélection en secret, d'un entier u et de deux grands nombres premiers p et q distincts et de taille voisine tels que u divise (p-1) et divise (q-1).
- calcul du nombre n égal au produit p.q;
- calcul du nombre $\lambda(n)=PPCM(p-1, q-1)$, c'est à dire de l'indicateur de Carmichael du nombre n;
- détermination d'un nombre h, $0 \leq h < n^2$, qui remplisse les deux conditions suivantes :

a) h est inversible modulo n^2 et

b) $ord(h,n^2)=0 \bmod n$.

- calcul du nombre $g= h^{\lambda(n)/u} \bmod n^2$.

La clé publique K est alors formée par le nombre n et le nombre g. La clé privée est constituée par les entiers (p,q,u) conservés secrètement dans le dispositif.

De préférence, on choisit h=2, lorsque c'est possible (c'est à dire si h=2 remplit les conditions a) et b), pour faciliter le calcul de g).

On notera que si u =PGCD(p-1,q-1), il n'est pas nécessaire de conserver ce nombre qui peut-être retrouvé par le dispositif à partir de p et q

De préférence, on choisira u premier, pour améliorer la sécurité du procédé, et de petite taille, typiquement 160

bits. En choisissant une petite taille pour u, on verra que l'on facilite le calcul de déchiffrement.

Dans ce troisième mode de réalisation, la mise en oeuvre du procédé de chiffrement pour chiffrer un message m est identique à celle précédemment décrite dans le premier mode de réalisation de l'invention, le cryptogramme étant égal à $c = g^m \bmod n^2$.

On peut aussi calculer le cryptogramme c en utilisant une variable aléatoire r selon la première variante du deuxième mode de réalisation de l'invention précédemment décrit. r est alors un entier aléatoire, de même taille que u et le cryptogramme est obtenu par le calcul suivant : $c=g^{m+nr} \bmod n^2$.

Le cryptogramme c calculé selon l'une ou l'autre mise en œuvre précédente du procédé de chiffrement est envoyé au dispositif B qui doit le déchiffrer. La mise en œuvre du procédé de déchiffrement par le dispositif B qui reçoit le message est un peu différente.

En effet, le calcul effectuĕ dans le dispositif dans une instance de déchiffrement, pour retrouver le nombre m à partir du cryptogramme c devient le suivant :

$$m = \frac{\log_n(c^u \bmod n^2)}{\log_n(g^u \bmod n^2)} \bmod n.$$

On peut appliquer comme précédemment des variantes de calcul qui permettent d'accélérer le temps de traitement nécessaire.

Dans une première variante, on va ainsi précalculer une fois pour toutes la quantité :

$\beta_{n,g}=\log_n(g^u \bmod n^2)^{-1} \bmod n$

et la conserver secrètement en mémoire.

Lors d'une instance de déchiffrement d'un cryptogramme c reçu, le dispositif n'a plus qu'à effectuer le calcul suivant :

$m=\log(c^u \bmod n^2)\cdot \beta_{n,g} \bmod n.$

Dans une deuxième variante, on met en oeuvre le Théorème du Reste Chinois, en utilisant les fonctions $\log_p$ et $\log_q$ déjà vues pour effectuer le calcul de déchiffrement.

Lors d'une instance de cette variante du procédé de déchiffrement du cryptogramme c reçu, le dispositif effectue alors les calculs suivants :

1. $m_p=\log_p(c^u \bmod p^2)\log_p(g^u \bmod p^2)^{-1} \bmod p$
2. $m_q=\log_q(c^u \bmod q^2)\log_q(g^u \bmod q^2)^{-1} \bmod q$
3. $m = TRC(m_p,m_q,p,q)$.

Dans une troisième variante, on accélère encore le temps de traitement nécessaire au déchiffrement du cryptogramme c selon la deuxième variante, en précalculant les quantités suivantes :

$\beta_{p,g}=\log(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g}=\log(g^u \bmod q^2)^{-1} \bmod q$

et en les conservant de façon secrète dans le dispositif.

Lors d'une instance de calcul de cette troisième variante du procédé de déchiffrement du cryptogramme c reçu, le dispositif n'a alors plus qu'à effectuer les calculs suivants :

1. $m_p=\log_p(c^u \bmod p^2)\ \beta_{p,g} \bmod p$
2. $m_q=\log_q(c^u \bmod q^2)\ \beta_{q,g} \bmod q$
3. $m = TRC(m_p,m_q,p,q)$.

Dans un quatrième mode de réalisation de l'invention, le procédé de chiffrement et le procédé de déchiffrement sont tels qu'ils présentent la particularité d'être des permutations sur le groupe des entiers modulo n^2. En d'autres termes, si le message m s'exprime sur k bits, le cryptogramme c obtenu en appliquant le procédé de

chiffrement sur m et la signature s obtenue en appliquant le procédé de déchiffrement sur m sont aussi sur k bits.

Cette particularité confère au procédé cryptographique la propriété supplémentaire de pouvoir être utilisé aussi bien en chiffrement/déchiffrement qu'en génération/vérification de signature. Dans ce cas, le procédé de déchiffrement est employé comme procédé de génération de signature et le procédé de chiffrement comme procédé de vérification de signature.

Dans ce quatrième mode de réalisation, le procédé de génération des clés publique et privée est le même que celui du premier mode de réalisation de l'invention : $K=(n,g)$ et $K'=(p,q,\lambda(n))$ ou $K'=(p,q)$.

Si le dispositif A veut envoyer un message m chiffré au dispositif B, il se procure la clé publique (n,g) de ce dernier, puis dans une instance du procédé de chiffrement, effectue alors les calculs suivants, appliqué au nombre m, $0 \leq m < n^2$:

1. $m_1 = m \bmod n$
2. $m_2 = (m-m1)/n$ (division euclidienne)
3. $c = g^{m1}\, m_2^{\,n} \bmod n^2$.

C'est ce cryptogramme c qui est envoyé au dispositif B.

Ce dernier doit donc lui appliquer le procédé de déchiffrement correspondant, pour retrouver m_1, m_2 et finalement m. Ce procédé de déchiffrement selon le quatrième mode de réalisation de l'invention consiste à effectuer les calculs suivants :

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w = cg^{-m1} \bmod n$.
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

Comme précédemment, des variantes du procédé de déchiffrement selon ce quatrième mode de réalisation de l'invention sont applicables, qui permettent de réduire le temps de traitement nécessaire pour déchiffrer un message donné. Elles sont intéressantes lorsque le dispositif a un grand nombre de cryptogrammes à déchiffrer.

Une première variante consiste à précalculer les quantités suivantes :

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ et

$\gamma_n = 1/n \bmod \lambda(n)$

que le dispositif B calcule une fois pour toutes et conserve secrètes en mémoire.

A chaque nouvelle instance de déchiffrement d'un cryptogramme c reçu selon cette première variante, le dispositif B n'a plus qu'à effectuer les calculs suivants :

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2)\ \alpha_{n,g} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^{\gamma_n} \bmod n$.
4. $m = m_1 + nm_2$.

Dans une deuxième variante de la mise en oeuvre du procédé de déchiffrement selon le quatrième mode de réalisation, on utilise le Théorème du Reste Chinois.

Le dispositif qui veut déchiffrer un cryptogramme c selon cette deuxième varainte effectue alors les calculs successifs suivants :

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2)\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$
7. $m_1=TRC(m_{1,p},m_{2,p},p,q)$.
8. $m2=TRC(m_{1,q},m_{2,q},p,q)$.

9. $m = m_1 + pqm_2$.

Dans une troisième variante, pour améliorer encore le temps de traitement du déchiffrement de cette deuxième variante, le dispositif B peut précalculer une fois pour toutes les quantités suivantes :

$\alpha_{p,g}=\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g}=\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

et les conserver secrètes en mémoire.

Le dispositif qui veut déchiffrer un cryptogramme c selon cette troisième varianten'a plus qu'à effectuer les calculs suivants:

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2)\ \alpha_{p,g} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{\gamma_p} \bmod p$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2)\ \alpha_{q,g} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{\gamma_q} \bmod q$
7. $m_1=TRC(m_{1,p},m_{2,p},p,q)$.
8. $m2=TRC(m_{1,q},m_{2,q},p,q)$.
9. $m = m_1 + pqm_2$.

Le quatrième mode de réalisation de l'invention qui vient d'être décrit permet de faire de la génération/ vérification de signature. Comme représenté sur l'organigramme de la figure 4, si le dispositif B doit générer une signature s d'un nombre m représentatif d'un message vers le dispositif A, il applique comme procédé de génération de la signature, le procédé de déchiffrement avec sa clé privée : $s=D_{K\cdot B}(m)$.

Le dispositif A qui reçoit la signature s et qui connaît le message m, vérifie que la signature est bonne en

calculant la quantité v obtenue en appliquant le procédé de chiffrement sur la signature s avec la clé publique : $v=E_{KB}(s)$. Si la signature est bonne, on a v=m.

Toutes les variantes de mise en oeuvre du procédé de déchiffrement de ce quatrième mode de réalisation qui permettent d'accélérer le temps de traitement sont aussi bien applicable en génération/vérification de signature.

L'invention qui vient d'être décrite est applicable dans tous les systèmes où l'on veut pouvoir chiffrer et/ou signer des messages. Elle permet d'élargir les possibilités d'adaptation aux différentes applications, selon que l'on recherche plus de sécurité, ou une vitesse de traitement accrue. A cet égard, on notera que le troisième mode de réalisation de l'invention, dont la complexité de calcul est seulement quadratique (fonction de n^2) offre un réel avantage en terme de vitesse, dans la mesure où tous les procédés de l'état de la technique ont un ordre de complexité supérieur (fonction de n^3). Un tel avantage intéresse plus particulièrement toutes les applications utilisant des dispositifs portables, tels les cartes à puces et plus particulièrement les dispositifs à bas coûts.

Enfin, toute personne expérimentée dans la technique concernée par l'invention comprendra que des modifications dans la forme et/ou des détails peuvent être effectués. En particulier on peut chiffrer la signature, ou encore appliquer une fonction de hachage au message m avant de calculer sa signature. Cela permet notamment d'avoir une signature différente à chaque fois même si le message m est inchangé.

REVENDICATIONS

1. Procédé cryptographique comprenant un procédé de génération de clés publique (K) et privée (K') dans un dispositif apte à échanger des messages sur au moins un canal de communication, la clé privée devant être conservée de façon secrète dans ledit dispositif et la clé publique devant être diffusée publiquement, le procédé de génération comprenant les étapes suivantes :

- sélection de deux nombres premiers p et q distincts, de taille voisine;
- calcul d'un nombre n égal au produit p.q;
- calcul du plus petit commun multiple des nombres (p-1) et (q-1) : $\lambda(n)=PPCM(p-1, q-1)$
- détermination d'un nombre g , $0 \leq g < n^2$ qui vérifie les deux conditions suivantes lors du calcul d'un cryptogramme c : $c = g^m \bmod n^2$:

a) g est inversible modulo n^2 et

b) $ord(g,n^2) = 1 \bmod n$,

la clé publique dudit dispositif étant formée par les paramètres n et g et sa clé privée étant formée par les paramètres p,q et $\lambda(n)$ ou par les paramètres p et q, procédé de génération, caractérisé en ce qu'il consiste à prendre g=2, si g vérifie les dites conditions a) et b).

2. Système de communication cryptographique à clés publique et privée générées selon la revendication 1, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant au moins une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif

(A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique (n_B, g_B) du deuxième dispositif (B) pour assigner aux paramètres n et g, les valeurs de la clé publique (n_B, g_B)
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

3. Système selon la revendication 2 , caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^{m+nr} \bmod (n^2)$,

4. Système selon la revendication 2, caractérisé en ce que le dispositif mettant en oeuvre le procédé de chiffrement comprend en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

-effectue le tirage d'un nombre entier aléatoire r, puis

-calcule le cryptogramme c en effectuant le calcul de chiffrement suivant: $c = g^m r^n \bmod (n^2)$.

5. Système selon la revendication 4, caractérisé en ce que le deuxième dispositif (B) met en oeuvre un procédé de déchiffrement, pour déchiffrer ledit cryptogramme c, et qui comprend la réalisation du calcul

$$m = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$$

x-1

où $\log_n(x) = \frac{\quad}{n}$

x étant un entier quelconque.

6. Système selon la revendication 5, caractérisé en ce qu'un dispositif (B) mettant en oeuvre ledit procédé de déchiffrement, précalcule la quantité :

$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$

et la conserve secrètement dans la zone sécurisée de la mémoire programme, x étant un entier quelconque.

7. Système selon la revendication 5, caractérisé en ce que dans une instance dudit procédé de déchiffrement un dispositif effectue les étapes de calcul suivantes, utilisant le Théorème du Reste Chinois TRC :

$m_p = \log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p.$

$m_q = \log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$

$m = TRC(m_p, m_q, p, q)$, où $\log_p$ et $\log_q$ sont tels que

$\log_i(x) = \frac{x-1}{i}$

x étant un entier quelconque.

8. Système selon la revendication 7, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ et

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q.$

et les conserve secrètement dans la zone sécurisée de la mémoire programme.

9. Système de communication cryptographique à clés publique et privée générées selon la revendication 1,

comprenant un canal de communication (20) et des dispositifs communiquant (A,B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n^2$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $K_B=(n_B,g_B)$ du deuxième dispositif (B) pour assigner aux paramètres n et g les valeurs de la clé publique (n_B, g_B).

- et réalisation des calculs suivants :

1. $m_1=m \bmod n$
2. $m_2=(m-m1)/n$
3. $c=g^{m1}\, m_2{}^n \bmod n^2$.

ledit cryptogramme c étant transmis sur le canal de communication vers le deuxième dispositif.

10. Système selon la revendication 9, caractérisé en ce que en ce que le deuxième dispositif (B) reçoit le cryptogramme c et met en oeuvre un procédé de déchiffrement, pour déchiffrer ledit cryptogramme ui comprend la réalisation des étapes suivantes de calcul :

1. $m_1=\log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$.
2. $w=cg^{-m1} \bmod n$.
3. $m_2=w^{1/n \bmod \lambda(n)} \bmod n$.
4. $m = m_1 + nm_2$.

11. Système selon la revendication 10, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement, précalcule les quantités suivantes :

$\alpha_{n,g}=\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$ et

$\gamma_n= 1/n \bmod \lambda(n)$

et les conserve secrètement dans la zone sécurisée de la mémoire programme.

12. Système selon la revendication 10, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif effectue les étapes de calcul suivant, en utilisant le Théorème du Reste Chinois :

1. $m_{1,p}=\log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$
2. $w_p=cg^{-m1,p} \bmod p$
3. $m_{2,p}=w_p^{1/q \bmod p-1} \bmod p.$
4. $m_{1,q}=\log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$
5. $w_q=cg^{-m1,q} \bmod q$
6. $m_{2,q}=w_q^{1/p \bmod q-1} \bmod q$
7. $m_1=TRC(m_{1,p},m_{2,p},p,q).$
8. $m2=TRC(m_{1,q},m_{2,q},p,q).$
9. $m = m_1 + pqm_2$, où $\log_p$ et $\log_q$ sont tels que

$$\log_i(x)= \frac{x-1}{i}$$

13. Système selon la revendication 12, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif précalcule les quantités suivantes :

$\alpha_{p,g}=\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g}=\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p= 1/q \bmod p-1$

$\gamma_q= 1/p \bmod q-1$

et les conserve secrètement dans la zone mémoire sécurisée de la mémoire programme.

14. Système selon l'une quelconque des revendications 10 à 13, dans lequel le procédé de déchiffrement est utilisé pour calculer la signature s d'un message m et le procédé de chiffrement est utilisé pour vérifier ladite signature.

15. Système de communication cryptographique à clés publique et privée générées selon la revendication 1, comprenant un canal de communication (20) et des dispositifs communiquant (A, B), chaque dispositif comprenant une interface de communication (11), des moyens de traitement de données (10) et des moyens de mémorisation (12, 13), caractérisé en ce qu'un procédé de chiffrement est mis en oeuvre dans un premier dispositif (A) pour envoyer un nombre m représentatif d'un message, $0 \leq m < n$, à un deuxième dispositif (B), ledit procédé de chiffrement comprenant les étapes suivantes :

- utilisation des paramètres de la clé publique $(n,g)_B$ du deuxième dispositif (B) pour assigner aux paramètres n et g les valeurs de la clé publique (n_B, g_B),
- calcul du cryptogramme $c = g^m \bmod n^2$,

ledit cryptogramme c étant ensuite transmis sur le canal de communication vers le deuxième dispositif.

16. Système selon la revendication 15, caractérisé en ce que le deuxième dispositif met en oeuvre le procédé de chiffrement comprenant en outre un générateur (15) d'un nombre entier aléatoire r, et en ce que ledit dispositif :

- effectue le tirage d'un nombre entier aléatoire r, puis,
- calcule le cryptogramme c en effectuant le calcul de chiffrement suivant : $c = g^{m+nr} \bmod (n^2)$

17. Système selon la revendication 15 ou 16, caractérisé en ce que le deuxième dispositif met en œuvre un procédé de déchiffrement du cryptogramme reçu c, comprenant la réalisation du calcul suivant :

$m = \log_n (c^u \bmod n^2).\log(g^u \bmod n^2)^{-1} \bmod n.$

18. Procédé selon la revendication 17, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule la quantité :

$\beta_{n,g}=\log_n(g^u \bmod n^2)^{-1} \bmod n$

et la conserve secrètement dans la zone sécurisé de la mémoire programme.

19. Système selon la revendication 17, caractérisé en ce que dans une instance dudit procédé de déchiffrement, un dispositif effectue les étapes de calcul suivantes, en utilisant le Théorème du reste chinois :

1. $m_p=\log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$.
2. $m_q=\log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$.
3. $m = TRC(m_p,m_q,p,q)$, où $\log_p$ et $\log_q$ sont tels que.

$$\log_i(x)=\frac{x-1}{i}$$

x étant en entier quelconque.

20. Système selon la revendication 19, caractérisé en ce qu'un dispositif mettant en oeuvre ledit procédé de déchiffrement précalcule les quantités suivantes :

$\beta_{p,g}=\log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g}=\log_n(g^u \bmod q^2)^{-1} \bmod q$

et les conserve secrètement dans la zone sécurisée de la mémoire programme.

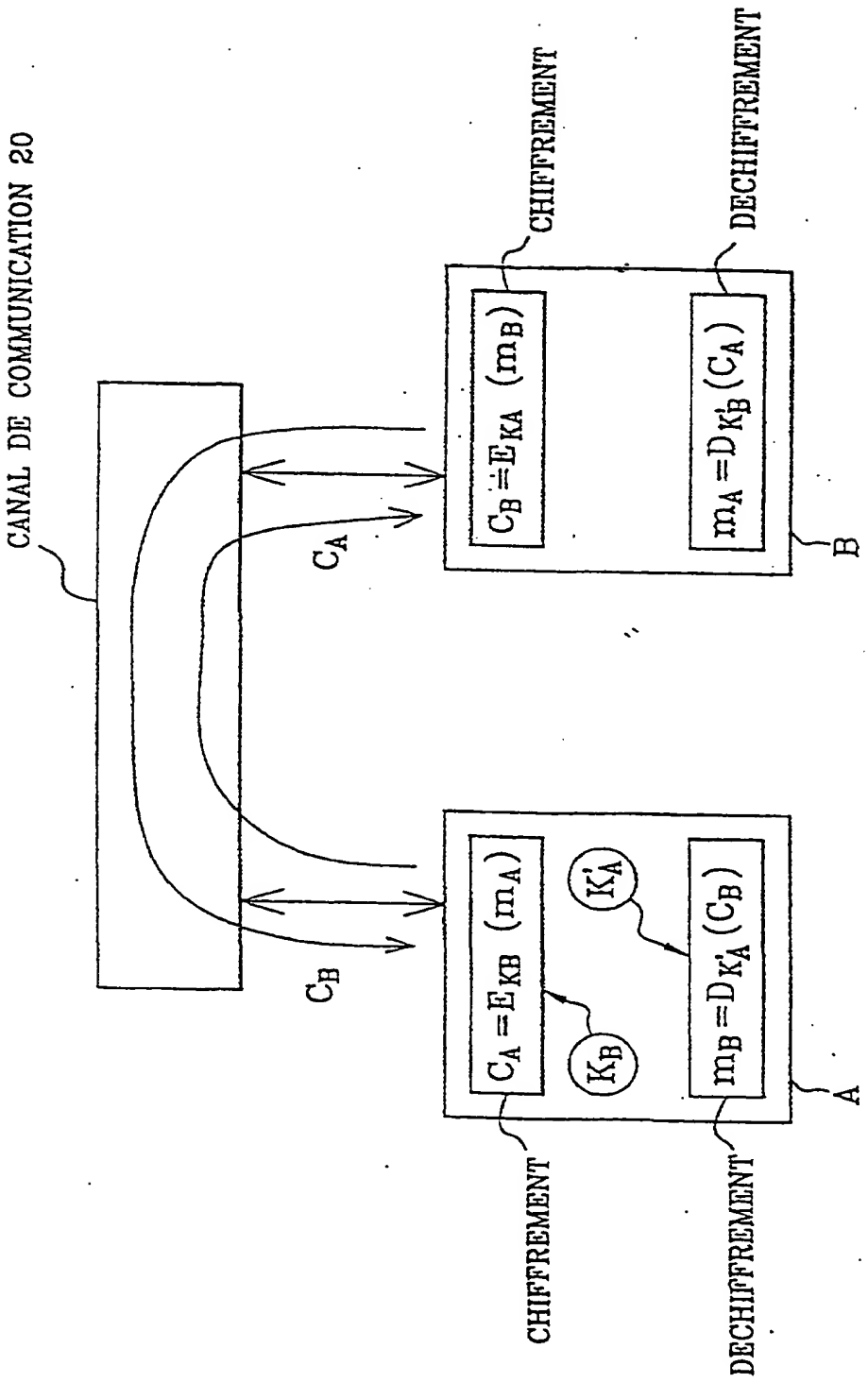

CANAL DE COMMUNICATION 20
CHIFFREMENT
DECHIFFREMENT
$C_B = E_{KA}(m_B)$
$m_A = D_{K'B}(C_A)$
B
C_A
C_B
$C_A = E_{KB}(m_A)$
$m_B = D_{K'A}(C_B)$
K_B
K'_A
A
CHIFFREMENT
DECHIFFREMENT

FIG.1